funkwerk
enterprise communications

Benutzerhandbuch

funkwerk S128p FastEthernet PoE Switch

Copyright © November 20, 2007 Funkwerk Enterprise Communications GmbH
Version 1.1

Ziel und Zweck

Dieses Dokument beschreibt die Installation und die Verwendung des **funkwerk S128p FastEthernet PoE Switch**.

Haftung

Der Inhalt dieses Dokuments wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Dokument gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Dokument können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Änderungen finden Sie unter www.funkwerk-ec.com.

Marken

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Alle Rechte sind vorbehalten. Kein Teil dieses Handbuchs darf ohne schriftliche Genehmigung der Firma Funkwerk Enterprise Communications GmbH in irgendeiner Form reproduziert oder weiterverwertet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Funkwerk Enterprise Communications GmbH nicht gestattet.

Richtlinien und Normen

Funkwerk Produkte entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EC

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.funkwerk-ec.com.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

Warnhinweis CE-Marke

Dies ist ein Produkt der Klasse A. Wenn es in einem Wohnbereich betrieben wird, kann es zu Funkstörungen führen, bei denen der Benutzer eventuell entsprechende Gegenmaßnahmen ergreifen muss.

1 Einleitung 7

2 Beschreibung der Hardware 15

2.1 Desktop-Installation 17

2.2 Anbringen der Gummifüße 17

2.3 Anschluss an die Netzspannung 18

3 Verwendung im Netzwerk 19

4 Konsolenmanagement 21

4.1 Login an der Konsolenschnittstelle 21

4.2 CLI-Management 23

4.3 Befehls-Level 24

4.4 Liste von Befehlen 26

4.5 Systembefehle 26

4.6 Portbefehle 29

4.7 Trunk-Befehle 33

4.8 VLAN-Befehle 34

4.9 Spanning-Tree-Befehle 37

4.10 QoS-Befehle 39

4.11 IGMP-Befehle 40

4.12 MAC- / Filtertabellenbefehle 41

4.13 SNMP-Befehle 42

4.14 Port-Mirroring-Befehle 45

4.15 802.1x-Befehle 45

4.16 TFTP-Befehle 48

4.17 System Log-, SMTP- und Ereignis-befehle 49
4.18 SNTP-Befehle 51
4.19 X-Ring-Befehle 53

5 Web-basiertes Management 55

5.1 Web-basiertes Management 55
5.2 Vorbereitung für Web Management 55
5.3 System Login 56
5.4 Systeminformationen 56
5.5 IP-Konfiguration 58
5.6 DHCP-Konfiguration 59
5.6.1 Konfiguration des DHCP-Servers 59
5.6.2 Einträge des DHCP Clients 60
5.6.3 Port und IP Binding 61
5.7 Update Firmware 61
5.8 Konfiguration wiederherstellen 62
5.9 Backup-Konfiguration 63
5.10 Konfiguration des System Log 64
5.11 SMTP-Konfiguration 65
5.12 Konfiguration von Ereignissen 66
5.13 SNTP-Konfiguration 68
5.14 IP-Sicherheit 70
5.15 Benutzerauthentifizierung 72
5.16 Portstatistik 73
5.17 Konfiguration der Portsteuerung 74

5.18 Port Trunk 75
5.18.1 Einstellungen zur Trunk-Gruppe 76
5.18.2 Informationen zur Leitungsbündelung 78
5.18.3 Aktivitätsstatus 78
5.19 Port Mirroring 80
5.20 Begrenzung der Bandbreite 81
5.21 VLAN-Konfiguration 83
5.21.1 Port-basiertes VLAN 84
5.21.2 802.1Q VLAN 86
5.22 Rapid Spanning Tree 89
5.22.1 RSTP-Systemkonfiguration 90
5.22.2 RSTP-Konfiguration pro Port 91
5.23 SNMP-Konfiguration 94
5.23.1 Systemkonfiguration 94
5.23.2 Trap-Konfiguration 95
5.23.3 SNMPv3-Konfiguration 96
5.24 QoS-Konfiguration 99
5.24.1 QoS-Policy und Prioritäten 99
5.24.2 Port-basierte Priorität 100
5.24.3 CoS-Konfiguration 101
5.24.4 ToS-Konfiguration 101
5.25 IGMP-Konfiguration 101
5.25.1 IGMP-Konfiguration 102
5.25.2 X-Ring 103
5.26 Sicherheitskonfiguration 105
5.26.1 802.1X-Konfiguration 105
5.26.2 Port-Sicherheit 109
5.27 Power-over-Ethernet 113

5.28 Standardeinstellungen 115
5.29 Konfiguration abspeichern 115
5.30 System neu starten 116

6 Fehlerbehebung 117

6.1 Falsch angeschlossene Verbindungen 117
6.2 Fehleranzeige durch LEDs 118

7 Technische Daten 119

8 Anhang 121

8.1 Pinbelegung am Konsolenport 121
8.2 Kabel 122
8.3 100BASE-TX/10BASE-T Pinbelegung 123
8.3.1 RJ-45 Pinbelegung von PD, die nicht dem 802.3af Standard PD entsprechen, mit feldkompatibler POE HUB RJ-45 Pinbelegung 123

1 Einleitung

Beim Einsatz von **Power-over-Ethernet** (PoE, Strom über das Ethernet) werden Geräte über eine Netzwerkverkabelung mit einer Netzspannung von 110/220 V Wechselstrom versorgt. Bei der Nutzung von Power-over-Ethernet wird bei der Systeminstallation nur ein einziges Cat. 5 Ethernetkabel benötigt, mit dem sowohl die Netzspannung, als auch Daten zu jedem Gerät transportiert werden. Dies bietet eine größere Flexibilität bei der Platzierung der Netzwerkgeräte und trägt in vielen Fällen erheblich zur Kostensenkung bei.

Bei PoE werden zwei Systemkomponenten eingesetzt: das Power Sourcing Equipment (PSE) liefert die Netzspannung und baut die Verbindung zur zweiten Komponente auf, dem Powered Device (PD), also dem Gerät, das mit der Netzspannung zu versorgen ist. Der Strom fließt über 2 der 4 Twisted-Pair-Adern des Cat. 5 Kabels.

Power-over-Ethernet ist konform zum IEEE 802.3af-Standard und ist vollkommen kompatibel zu den marktüblichen Ethernet Switches und Netzwerkgeräten. Das Power Sourcing Equipment (PSE), welches die Netzspannung liefert, prüft, ob das Netzwerkgerät PoE-fähig ist. Das bedeutet, Strom fließt erst dann, wenn festgestellt wurde, dass ein Powered Device am anderen Ende des Kabels angeschlossen ist. Darüber hinaus überwacht das PSE den Übertragungskanal. Nimmt das Powered Device, also das zu speisende Gerät, nicht eine Mindestnetzspannung ab, weil es ausgesteckt oder ausgeschaltet wurde, dann stellt das PSE die Stromzufuhr zu diesem Port ab. Optional gestattet es der Standard den Powered Devices, den PSEs zu signalisieren, wieviel Netzspannung von ihnen benötigt wird.

Der **funkwerk S128p FastEthernet PoE Switch** ist ein Multi-Port-Switch, mit dem hochleistungsfähige, geswitchte Workgroup-Netzwerke aufgebaut werden können. Der Switch ist ein Gerät, das Store-and-Forward-Switching ermöglicht und niedrige Latenzzeiten für Hochgeschwindigkeits-Netzwerke bietet. Der Switch verfügt über ein Schema für Store-and-Forward-Switching. Dies ermöglicht es dem Switch, Auto-Learning zu betreiben und Quelladressen in einer MAC-Adresstabelle mittels 8 K Einträgen zu speichern. Der Switch wurde zum Betrieb in Netzwerken für Workgroups, Abteilungen oder in Backbones entwickelt. Der funkwerk S128p FastEthernet PoE Switch verfügt über 8 10/100Base-TX RJ-45 Ports (4 Ports bieten PoE-Funktionalität) mit Auto-Sen-

sing und über 1 Giga-Kupfer-Port mit 1 Mini-GBIC-Steckplatz für höhere Datenraten.

Leistungsmerkmale

- 8-Port 10/100TX und 1 Gigabit Port (wahlweise RJ45 Mini GBIC)
- 4 Ports mit integrierter PoE-Funktion
- Konform zu IEEE802.3 10BASE-T, 802.3u 100BASE-TX, 802.3z Gigabit Glasfaser, IEEE 802.3ab 1000Base-T und IEEE 802.3af
- Switch mit 5,6 Gbit/s Bandbreite
- 802.1p CoS, 4 Queues pro Port
- IGMP Snooping und Unterstützung des Query Modes (Abfragemodus) für Multimedia-Applikationen
- Unterstützt die GVRP-Funktion
- Broadcast-Storm-Filter
- TFTP Firmware Update
- SNMP/Web/Telnet/CLI Management
- Bandbreitenkontrolle pro Port
- Sicherheitsfunktionalität zum Management von IP-Adressen
- Port-basiertes VLAN /802 .1Q VLAN
- IEEE802.3ad Port Trunk mit LACP
- IEEE802.3x Flow Control
  - Vollduplex Flow Control
  - Halbduplex-Back-Pressure-Verfahren
- Port Mirror und Bandbreitenkontrolle
- Spanning Tree Protokoll
  - STP / Rapid STP
- QoS für die untenstehende Methode:
  - Port-basiert / Tag-basiert

  - IPv4 ToS/ Ipv4, IPv6 DiffServ
- IEEE 802.1x Benutzerauthentisierung
- DHCP Client, Server
- Unterstützung von SNTP und SMTP
- Sicherheitsfunktionalität für MAC-Adressen
- Unterstützung von SNMP Trap
- Upload und Download von Konfigurationen
- Unterstützung von X-Ring

Leistungsmerkmale der Software

MANAGEMENT	SNMP v1, SNMP v2c, SNMP v3, Telnet, Konsole (CLI), Web und Menü-gesteuertes** Management.
RFC STANDARD	RFC2233 MIBII, RFC 1157 SNMP MIB, RFC 1493 Bridge MIB, RFC 2674 VLAN MIB, RFC 2665 Ethernet like MIB, RFC1215 Trap MIB, RFC 2819 RMON MIB, Private MIB, RFC2030 SNTP, RFC 2821 SMTP, RFC 1757 RMON1 MIB, RFC 1215 Trap
SNMP TRAP	Kaltstart, Warmstart, Link down, Link up, Autorisierung fehlgeschlagen, SNMP Trap an bis zu 3 Stationen
SOFTWARE UPGRADE	TFTP Firmware Upgrade
PORT TRUNK	Unterstützt IEEE802.3ad mit LACP-Funktion. Bis zu 3 Trunk-Gruppen, maximale Anzahl von Gruppenmitgliedern bis zu 4 Ports.
SPANNING TREE	Spanning Tree

VLAN	Port-basiertes VLAN Double Tag VLAN (Q in Q)* IEEE802.1Q Tag VLAN. Es können bis zu 256 statische und bis zu 2048 dynamische VLAN-Gruppen konfiguriert werden. Die möglichen VLAN IDs reichen von 1 bis 4094. GVRP-Funktion unterstützt 256 Gruppen.
CLASS OF SERVICE	Pro Port werden bis zu 4 Queues (Warteschlangen) unterstützt. Weight Round Ratio (WRR): hoch: mittel bis hoch: mittel bis niedrig: niedrig (8:4:2:1)
QUALITY OF SERVICE	Port-basiert, Tag-basiert, Servicetyp gemäß IPv4, andere Dienste gemäß IPv6
IGMP	Konform zu IGMP v1 und v2; unterstützt weiterhin 256 IGMP-Gruppen sowie den Query Mode (Abfragemodus).
PORT-SICHERHEIT	Unterstützt Filter für eingehende und ausgehende MAC-Adressen und die Blockierung statischer MAC-Quelladressen.
PORT MIRROR	System unterstützt 3 Mirroring-Typen: "RX, TX und beide Paketarten". Die maximale Anzahl von Port-Mirror-Einträgen ist 8.
BANDBREITENKONTROLLE	Die Datenrate für eingehende Datenpakete begrenzt die Paketart: alle Frames, Broadcast, Multicast, unbekannte Unicast- und Brodcast-Pakete Die Anpassung der Datenrate für die ausgehenden Datenpakete unterstützt alle Arten von Paketen. Schwellenwerte, welche die Datenrate begrenzen: 64 kbit/s bis 64 Mbit/s oder bis zu 256 Mbit/s für Gigabit Port.

BENUTZER-AUTHENTISIERUNG	Unterstützt IEEE802.1x Benutzerauthentisierung und versendet Meldungen an den RADIUS-Server. – Abweisen – Annehmen – Autorisieren – Abschalten
DHCP	DHCP-Client und DHCP-Server. Stellen einen globalen IP-Adresspool für den DHCP-Server bereit.
PAKETFILTER	Broadcast Storm Paketfilter
PORT-SICHERHEIT	Sicherheitsfunktionalität für eingehende und ausgehende MAC-Adresse. Pro Port werden 50 MAC-Adressen unterstützt. Begrenzung der Anzahl der Port-MAC-Adressen. Pro Port werden 50 MAC-Adressen unterstützt.
SNMP IP SICHERHEIT	Unterstützt 10 IP Adresskonten für ein Sicherheitsmanagementsystem für Web und SNMP, Telnet-Sicherheitsmanagement zum Schutz gegen unerlaubtes Eindringen ins Netzwerk.
SYTEMPROTOKOLL	Unterstützt Remote Log Server. Stellt 1000 Protokolleinträge bereit.
SNTP	Unterstützt RFC2030 Simple Network Time Protocol.
SMTP	5 Mail Accounts
UPLOAD UND DOWNLOAD VON KONFIGURATIONEN	Unterstützt Konfigurationsdateien im Binärformat zur schnellen Installation von Systemen.
X-RING	Stellt redundante Backup-Features zu X-Ring, Dual Homing und Couple Ring bereit und bietet eine Wiederherstellungszeit von weniger als 300 ms.

PoE Management	***PoE Enable/Disable: (PoE: Einschalten/Ausschalten:)***Funktion zum Ein- und Ausschalten von PoE. ***Power limit by classification: (Beschränkung der Netzspannung durch Klassifizierung:)*** Einschalten/Ausschalten der Klassifizierung der Netzspannung des PD. Die Ausgangsleistung wird durch die Klassifizierung des PD begrenzt. ***Power limit by management: (Beschränkung der Netzspannung durch Management:)*** Einschalten der Priorisierung der Stromzufuhr. ***Priority (Priorität)***: Prioritätseinstellungen zur Stromzufuhr pro Port. Wenn die Ausgangsleistung den Switch verlässt, dann wird die Stromzufuhr bei niedriger Priorität des Ports abgestellt. ***Detect Legacy Signature (Legacy-Signature erkennen):*** Das Ziel der Erkennung einer Legacy-Signatur ist es, die Geräte auf der Basis ihrer eindeutigen, elektrischen Signaturen (widerstandsseitig und kapazitiv) zu erkennen und sie möglichst selektiv mit Netzspannung zu versorgen. Einige dieser CISCO-PD-Geräte wurden vor Verabschiedung des Standards entwickelt und entsprechen nicht dem Standard 802.3af bezüglich einer exakten elektrischen Signatur. In solchen Fällen muss diese Funktion abgeschaltet werden.

Lieferumfang

Packen Sie den Packungsinhalt des **funkwerk S128p FastEthernet PoE Switch** aus und vergleichen Sie die Komponenten mit der untenstehenden Checkliste.

- **funkwerk S128p FastEthernet PoE Switch**
- RS-232-Kabel
- 4 Gummifüße
- Stromkabel
- Benutzerhandbuch

Bitte vergleichen Sie den Packungsinhalt Ihres **funkwerk S128p FastEthernet PoE Switch** mit dem oben angegebenen Lieferumfang. Wenn ein Teil fehlt oder beschädigt ist, wenden Sie sich bitte an Ihren Händler.

2 Beschreibung der Hardware

Dieser Abschnitt beschreibt die Hardware des **funkwerk S128p FastEthernet PoE Switch** und gibt einen Überblick über den Aufbau und die Funktionsweise des Switch.

Physikalische Abmessungen

Die physikalischen Abmessungen des **funkwerk S128p FastEthernet PoE Switch** sind *217mm (Breite) x 140mm (Tiefe) x 43mm (Höhe)*.

Vorderseite

An der Vorderseite des **funkwerk S128p FastEthernet PoE Switch** befinden sich 8 10/100Base-TX RJ-45 Ethernet Ports (Auto MDI/MDIX), 1 Giga Port und 1 Mini GBIC Port. Die LEDs sind ebenso an der Vorderseite des Switch angebracht.

Abbildung 2-1: Vorderseite des **funkwerk S128p FastEthernet PoE Switch**

- **RJ-45 Ports:** 8x 10/100 N-Way Auto-Sensing für 10Base-T- oder 100Base-TX-Verbindungen. 4 dieser RJ-45 Ports liefern die Netzspannung für die strombetriebenen Geräte über eine MDI (Media-Dependent Interface, medienabhängige Schnittstelle).
  MDI beinhaltet im Allgemeinen den Aufbau einer Verbindung zu einem anderen Hub oder Switch, während **MDIX** den Aufbau einer Verbindung zu einem anderen Endgerät oder einem anderen PC meint. Das Leistungsmerkmal **Auto MDI/MDIX** bietet Ihnen die Möglichkeit, eine Verbindung zu einem anderen Switch oder einem Endgerät aufzubauen, ohne ein Kreuzkabel verwenden zu müssen.
- **1 Giga Port:** 1 x 10/100/1000TX N-Way Auto-Sensing für eine 10/100/1000-Verbindung.
- **1 Mini GBIC Port:** 1 Mini GBIC Port für eine Gigabit-Glasfaserverbindung.

LED-Anzeigen Die LED-Anzeigen geben Auskunft über den jeweiligen Betriebszustand des Geräts. Die untenstehende Tabelle beschreibt die verschiedenen Zustände der LEDs und die entsprechenden Bedeutungen.

LED	Status	Beschreibung
Power (Netzspannung)	Grün	Anschluss an die Netzspannung
	Aus	Netzspannung nicht vorhanden
1000M (Port 9)	Grün	Datenrate: 1.000 Mbit/s
	Orange	Datenrate: 100 Mbit/s
	Aus	Kein Gerät angeschlossen
FWD (Port 5 - 8)	Grün	Der Port liefert die vom Gerät benötigte Netzspannung.
	Aus	Es ist kein Gerät angeschlossen oder es liegt keine Netzspannung an.
100M (Port 1 - 9)	Grün	Der Port arbeitet mit einer Datenübertragungsrate von 100 Mbit/s.
	Aus	Kein Gerät angeschlossen
LNK/ACT	Grün	Ein Gerät ist an den Port angeschlossen.
	Blinkt	Es findet eine Datenübertragung auf diesem Port statt.
	Aus	Kein Gerät angeschlossen
FDX/COL	Orange	Der Port arbeitet im Vollduplex-Modus.
	Blinkt	Es ist eine Kollision von Datenpaketen aufgetreten.
	Aus	Halbduplex-Modus

Rückseite Die Buchse für den Netzanschluss befindet sich auf der Rückseite des funkwerk S128p FastEthernet PoE Switch, wie in der Abbildung dargestellt. Der Switch arbeitet mit Wechselstrom in einem Spannungsbereich von 100 - 240 V Wechselstrom und in einem Frequenzbereich von 50 - 60 Hz.

Abbildung 2-2: Rückseite des **funkwerk S128p FastEthernet PoE Switch**

2.1 Desktop-Installation

Stellen Sie den Switch auf eine ausreichend große und ebene Fläche in der Nähe einer Steckdose. Die Fläche, auf die Sie den Switch stellen, muss sauber, glatt, eben und fest sein. Stellen Sie sicher, dass um den Switch herum ausreichend Freiraum ist, um Kabel anschließen zu können und eine ausreichende Luftzirkulation um das Gerät herum zu gewährleisten.

2.2 Anbringen der Gummifüße

1. Stellen Sie sicher, dass die Unterseite des Switch fett- und staubfrei ist.
2. Entfernen Sie die Schutzfolie von den Gummifüßen.
3. Bringen Sie die Gummifüße an den markierten Stellen an der Unterseite des Switch an. Diese Füße verhindern, dass der Switch bei Erschütterung oder Vibrationen umfällt.

2.3 Anschluss an die Netzspannung

1. Stecken Sie das Stromkabel in die dafür vorgesehene Buchse an der Rückseite des Switch. Stecken Sie das andere Ende des Stromkabels in eine Steckdose. Das integrierte Netzteil des Switch arbeitet in einem Spannungsbereich von 100 – 240 V Wechselstrom und einem Frequenzbereich von 50 - 60 Hz.
2. Überprüfen Sie die LED-Stromanzeige (Power) an der Vorderseite des Geräts. Sie zeigt Ihnen, ob das Gerät korrekt an die Stromversorgung angeschlossen wurde.

3 Verwendung im Netzwerk

PCs, Endgeräte und Server können miteinander kommunizieren, indem sie eine direkte Verbindung zum funkwerk S128p FastEthernet PoE Switch aufbauen. Der Switch lernt automatisch die Adressen der Knoten und verwendet diese anschließend, um den gesamten Datenverkehr, der an die Zieladressen gerichtet ist, zu filtern und weiterzuleiten.

Der Switch kann den Uplink Port benutzen, um eine Verbindung zu einem anderen Switch oder Hub aufzubauen und andere, kleinere, geswitchte Workgroup-Netzwerke anzubinden. Auf diese Art und Weise werden größere, geswitchte Netzwerke aufgebaut. Gemäß dem heutigen Stand der Technik können Glasfaserports verwendet werden, um Switche anzuschließen. Der PoE Switch liefert Netzspannung auf die UTP-Kabel. So werden die PDs (Powered Devices) mit der Netzspannung versorgt, die sie zum Betrieb benötigen.

Der 4-Port Power-over-Ethernet-Switch liefert die Netzspannung für die PDs, die gemäß Standard IEEE 802.3af im Netzwerk betrieben werden. Auf diese Art und Weise können Probleme bei der Anordnung von Geräten behoben werden. Das Netzwerkgerät kann in einer günstigeren Position platziert werden und so mehr Leistung bringen.

Hinweis

Wenn Sie den 4-Port Power-over-Ethernet-Switch mit dem Cisco Aironet 350 verbinden möchten, verwenden Sie dazu bitte ein **Kreuzkabel**. Für Geräte von anderen Herstellern verwenden Sie bitte **Non-Crossover-Kabel.**

4 Konsolenmanagement

4.1 Login an der Konsolenschnittstelle

Nachdem die Verbindung zwischen PC und Switch aufgebaut wurde, schalten Sie den PC an und starten ein Terminal-Emulationsprogramm oder das Programm **Hyper Terminal**. Konfigurieren Sie die Kommunikationsparameter. Sie sollten mit den folgenden Kennwerten für den Konsolenport übereinstimmen:

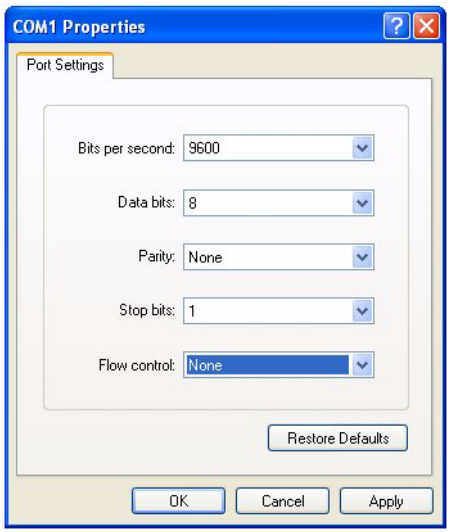


Abbildung 4-1: Einstellungen für die Kommunikationsparameter

***BAUD RATE (ÜBERTRAGUNGSRATE)**: 9600 bit/s*

***DATA BITS (DATENBITS)**: 8*

***PARITY (PARITÄT)**: None (keine)*

***STOP BIT**: 1*

***FLOW CONTROL**: None (keine)*

Nachdem Sie die Einstellungen für die Parameter eingegeben haben, klicken Sie auf "**OK**". Wenn daraufhin ein leerer Bildschirm dargestellt wird, drücken Sie die Enter-Taste, um das Login-Menü aufzurufen. Geben Sie den Standard-Benutzernamen "**admin**" und das Passwort "**funkwerk**" ein (benutzen Sie die **Enter**-Taste, um von einem Eingabefeld ins nächste zu gelangen). Drücken Sie dann die Enter-Taste. Danach erscheint das Konsolenmanagement-Menü. Die untenstehende Abbildung zeigt den Anmeldebildschirm.

Abbildung 4-2: Konsolen-Anmeldebildschirm

4.2 CLI-Management

Das System unterstützt zwei Arten von Konsolenmanagement – CLI-Befehle und Auswahl über das Menü. Nachdem Sie sich am System angemeldet haben, sehen Sie eine Eingabeaufforderung für einen Befehl. Um auf die CLI-Management-Oberfläche zu gelangen, geben Sie den Befehl **enable** ein. Die folgende Tabelle listet die CLI-Befehle auf und beschreibt sie.

Abbildung 4-3: CLI-Befehlsschnittstelle

4.3 Befehls-Level

Modus	Zugriffs-methode	Eingabe-aufforde-rung	Beenden durch	Zu diesem Modus
User EXEC	Starten Sie eine Sitzung mit Ihrem Switch.	switch>	Geben Sie "logout" oder "quit" ein.	Die Benutzerbefehle, die auf dem Benutzer-Level verfügbar sind, sind eine Untergruppe der Befehle, die auf dem privilegierten Level angeboten werden. Sie können diesen Modus nutzen, um ■ grundlegende Tests durchzuführen. ■ Systeminformationen anzuzeigen.
Privileged EXEC	Geben Sie "enable" ein, während Sie sich im User EXEC Modus befinden.	switch#	Geben Sie "disable" ein, um den Modus zu beenden.	Der Privileged Modus ist ein erweiterter Modus. Sie können den privilegierten Modus nutzen, um ■ den Status von erweiterten Funktionen anzuzeigen. ■ Konfigurationen abzuspeichern.
Global Configuration	Geben Sie diesen Befehl ein, während Sie sich im Privileged EXEC Modus befinden.	switch (config)#	Um diesen Modus zu verlassen und zum Privileged EXEC Modus zurückzukehren, geben Sie "exit" oder "end" ein.	Benutzen Sie diesen Modus, um Parameter zu konfigurieren, die für Ihren Switch insgesamt gelten.

Modus	Zugriffs-methode	Eingabe-aufforde-rung	Beenden durch	Zu diesem Modus
VLAN database	Geben Sie den Befehl "vlan data-base" ein, während Sie sich im Privile-ged EXEC Modus befin-den.	switch (vlan)#	Um diesen Modus zu ver-lassen und zum User EXEC Modus zurück-zukehren, geben Sie "exit" ein.	Nutzen Sie diesen Modus, um VLAN-spezifische Parameter zu konfigurieren.
Interface configuration	Geben Sie den „inter-face“-Befehl ein (mit einer spezifischen Schnittstelle), während Sie sich im Global Configuration Modus befin-den.	switch (config-if)#	Um diesen Modus zu ver-lassen und zum Global Configu-ration Modus zurückzukeh-ren, geben Sie "exit" ein. Um zum Privileged EXEC Modus zurückzukeh-ren, geben Sie "end" ein.	Nutzen Sie diesen Modus, um Para-meter für den Switch und den Ether-net Port zu konfigurieren.

4.4 Liste von Befehlen

USER EXEC	*E*
PRIVILEGED EXEC	*P*
GLOBAL CONFIGURATION	*G*
VLAN DATABASE	*V*
INTERFACE CONFIGURATION	*I*

4.5 Systembefehle

Befehl	Stufe	Beschreibung	Beispiel
`show config`	*E*	Zeigt die Switchkonfiguration an.	*switch>show config*
`show terminal`	*P*	Zeigt Konsoleninformationen an.	*switch#show terminal*
`write memory`	*P*	Speichert die Benutzerkonfiguration in einem permanenten Speicher ab (Flash Rom).	*switch#write memory*
`system name [System Name]`	*G*	Konfiguriert den Systemnamen.	*switch(config)#system name xxx*
`system location [System Location]`	*G*	Legt den Lokations-String für das Switch-System fest.	*switch(config)#system location xxx*
`system description [System Description]`	*G*	Legt den Beschreibungs-String für das Switch-System fest.	*switch(config)#system description xxx*

Befehl	Stufe	Beschreibung	Beispiel
`system contact [System Contact]`	*G*	Legt den Contact Window String für das Switch-System fest.	*switch(config)#system contact xxx*
`show system-info`	*E*	Zeigt Systeminformationen an.	*switch>show system-info*
`ip address [Ip-address] [Subnet-mask] [Gateway]`	*G*	Konfiguriert die IP-Adresse des Switch.	*switch(config)#ip address 192.168.1.1 255.255.255.0 192.168.1.254*
`ip dhcp`	*G*	Aktiviert die DHCP-Client-Funktion des Switch.	*switch(config)#ip dhcp*
`show ip`	*P*	Zeigt IP-Informationen zum Switch an.	*switch#show ip*
`no ip dhcp`	*G*	Deaktiviert die DHCP-Client-Funktion des Switch.	*switch(config)#no ip dhcp*
`reload`	*G*	Hält alle Prozesse an und führt einen Kaltneustart durch.	*switch(config)#reload*
`default`	*G*	Setzt System auf Default-einstellungen zurück.	*switch(config)#default*
`admin username [Username]`	*G*	Ändert einen Login-Benutzernamen (maximal 10 Zeichen).	*switch(config)#admin username xxxxxx*
`admin password [Password]`	*G*	Legt ein Passwort fest (maximal 10 Zeichen).	*switch(config)#admin password xxxxxx*
`show admin`	*P*	Zeigt Administratorinformationen an.	*switch#show admin*
`dhcpserver enable`	*G*	Aktiviert den DHCP-Server.	*switch(config)#dhcpserver enable*
`Dhcpserver disable`	*G*	Deaktiviert den DHCP-Server.	*switch(config)#no dhcpserver*

Befehl	Stufe	Beschreibung	Beispiel
`dhcpserver lowip [Low IP]`	*G*	Konfiguriert niedrige IP-Adresse für IP-Pool.	*switch(config)#dhcpserver lowip 192.168.1.100*
`dhcpserver highip [High IP]`	*G*	Konfiguriert hohe IP-Adresse für IP-Pool.	*switch(config)#dhcpserver highip 192.168.1.200*
`dhcpserver subnetmask [Subnet mask]`	*G*	Konfiguriert Subnetzmaske für DHCP-Clients.	*switch(config)#dhcpserver subnetmask 255.255.255.0*
`dhcpserver gateway [Gateway]`	*G*	Konfiguriert Gateway für DHCP-Clients.	*switch(config)#dhcpserver gateway 192.168.1.254*
`dhcpserver dnsip [DNS IP]`	*G*	Konfiguriert DNS IP für DHCP-Clients.	*switch(config)#dhcpserver dnsip 192.168.1.1*
`dhcpserver leasetime [Hours]`	*G*	Konfiguriert die Lease Time (in Stunden).	*switch(config)#dhcpserver lease-time 1*
`dhcpserver ipbinding [IP address]`	*I*	Legt eine statische IP-Adresse für DHCP-Clients nach Port an.	*switch(config)#interface fastEthernet 2switch(config)#dhcpserver ipbinding 192.168.1.1*
`show dhcpserver configuration`	*P*	Zeigt die Konfiguration des DHCP-Servers an.	*switch#show dhcpserver configuration*
`show dhcpserver clients`	*P*	Zeigt Client-Einträge auf dem DHCP-Server an.	*switch#show dhcpserver clients*
`show dhcpserver ip-binding`	*P*	Zeigt die IP-Adressen-Zuordnung des DHCP-Servers zu den jeweiligen Ports an.	*switch#show dhcpserver ip-binding*
`no dhcpserver`	*G*	Deaktiviert die DHCP-Server-Funktion.	*switch(config)#no dhcpserver*
`security enable`	*G*	Aktiviert die IP-Sicherheitsfunktion.	*switch(config)#security enable*
`security http`	*G*	Aktiviert die IP-Sicherheitsfunktion des HTTP-Servers.	*switch(config)#security http*

Befehl	Stufe	Beschreibung	Beispiel
`security telnet`	*G*	Aktiviert die IP-Sicherheitsfunktion des Telnet-Servers.	*switch(config)#security telnet*
`security ip [Index(1..10)] [IP Address]`	*G*	Legt die IP-Sicherheitsliste fest.	*switch(config)#security ip 1 192.168.1.55*
`show security`	*P*	Zeigt Informationen zur IP-Sicherheit an.	*switch#show security*
`no security`	*G*	Deaktiviert die IP-Sicherheitsfunktion.	*switch(config)#no security*
`no security http`	*G*	Deaktiviert die IP-Sicherheitsfunktion des HTTP-Servers.	*switch(config)#no security http*
`no security telnet`	*G*	Deaktiviert die IP-Sicherheitsfunktion des Telnet-Servers.	*switch(config)#no security telnet*

4.6 Portbefehle

Befehl	Stufe	Beschreibung	Beispiel
`interface fastEthernet [Portid]`	*G*	Wählen Sie den Port aus, auf dem Änderungen vorgenommen werden sollen.	*switch(config)#interface fastEthernet 2*
`duplex [full | half]`	*I*	Verwenden Sie den "duplex"-Konfigurationsbefehl, um den Duplexmodus für den Betrieb mit FastEthernet festzulegen.	*switch(config)#interface fastEthernet 2 switch(config-if)#duplex full*

Befehl	Stufe	Beschreibung	Beispiel
`speed [10|100|1000|auto]`	*I*	Verwenden Sie den Schnell-Konfigurationsbefehl, um den Hochgeschwindigkeitsmodus für den Betrieb mit Fast Ethernet festzulegen. Die Geschwindigkeit kann nicht auf 1000 eingestellt werden, wenn der Port kein Giga-Port ist.	*switch(config)#interface fastEthernet 2* *switch(config-if)#speed 100*
`no flowcontrol`	*I*	Deaktiviert Flow Control für die Schnittstelle.	*switch(config-if)#no flowcontrol*
`security enable`	*I*	Aktiviert die Sicherheitsfunktion der Schnittstelle.	*switch(config)#interface fastEthernet 2* *switch(config-if)#security enable*
`no security`	*I*	Deaktiviert die Sicherheitsfunktion der Schnittstelle.	*switch(config)#interface fastEthernet 2* *switch(config-if)#no security*
`bandwidth type all`	*I*	Setzt die Begrenzung für Frame-Typen an der eingehenden Schnittstelle auf "accept all frames (Akzeptiere alle Frames)".	*switch(config)#interface fastEthernet 2switch(config-if)#bandwidth type all*
`bandwidth type broadcast-multicast-flooded-unicast`	*I*	Setzt die Begrenzung für Frame-Typen an der eingehenden Schnittstelle auf "accept broadcast, multicast, and flooded unicast frames (Akzeptiere Broadcast, Multicast und Flooded Unicast Frames)".	*switch(config)#interface fastEthernet 2* *switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast*

Befehl	Stufe	Beschreibung	Beispiel
`bandwidth type broadcast-multicast`	*I*	Setzt die Begrenzung für Frame-Typen an der eingehenden Schnittstelle auf "accept broadcast and multicast frames (Akzeptiere Broadcast und Multicast Frames)".	*switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast*
`bandwidth type broadcast-only`	*I*	Setzt die Begrenzung für Frame-Typen an der eingehenden Schnittstelle auf "only accept broadcast frames (Akzeptiere nur Broadcast Frames)".	*switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only*
`bandwidth in [Value]`	*I*	Legt die Eingangsbandbreite der Schnittstelle fest. Die Bandbreite reicht von 100kbit/s bis 256.000 kbit/s für Giga-Ports. 0 bedeutet, es gibt keine Begrenzung.	*switch(config)#interface fastEthernet 2switch(config-if)#bandwidth in 100*
`bandwidth out [Value]`		Legt die Ausgangsbandbreite der Schnittstelle fest. Die Bandbreite reicht von 100kbit/s bis 102.400 kbit/s oder 256.000 kbit/s für Giga-Ports. 0 bedeutet, es gibt keine Begrenzung.	*switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100*
`show bandwidth`	*I*	Zeigt die Bandbreitenkontrolle für die Schnittstelle an.	*switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth*

Befehl	Stufe	Beschreibung	Beispiel
`state [Enable | Disable]`	*I*	Verwenden Sie den „state“-Schnittstellenkonfigurations-befehl, um den Status der Ethernet-Ports festzulegen. Sie können diesen Befehl in der Variante zum Deaktivieren benutzen, um den Port zu deaktivieren.	*switch(config)#interface fastEthernet 2* *switch(config-if)#state Disable*
`show interface configuration`	*I*	Zeigt den Status der Konfiguration der Schnittstelle.	*switch(config)#interface fastEthernet 2* *switch(config-if)#show interface configuration*
`show interface status`	*I*	Zeigt den aktuellen Status der Schnittstelle.	*switch(config)#interface fastEthernet 2switch(config-if)#show interface status*
`show interface accounting`	*I*	Zeigt den Statistikzähler der Schnittstelle.	*switch(config)#interface fastEthernet 2* *switch(config-if)#show interface accounting*
`no accounting`	*I*	Löscht die Abrechnungsinformationen der Schnittstelle.	*switch(config)#interface fastEthernet 2* *switch(config-if)#no accounting*

4.7 Trunk-Befehle

Befehl	Stufe	Beschreibung	Beispiel
`aggregator priority[1-65535]`	*G*	Legt die Systempriorität der Portgruppe fest.	*switch(config)#aggregator priority 22*
`aggregator activityport [Group ID] [Port Numbers]`	*G*	Legt die Aktivität auf dem Port fest.	*switch(config)#aggregator activityport 2*
`aggregator group [GroupID] [Port-list] lacp workp [Workport]`	*G*	Weist einer Trunk-Gruppe aktives LACP zu. ***[GROUPID]*** : 1 - 3 ***[PORT-LIST]***: Liste von Member Ports. Dieser Wert kann eine Bandbreite von Ports (ex. 1 - 4) oder eine durch Kommas getrennte Portliste sein (ex. 2, 3, 6). ***[WORKPORT]:*** Anzahl der Work Ports. Der Wert darf nicht kleiner als 0 sein und nicht größer als die Anzahl von Member Ports.	*switch(config)#aggregator group 1 1-4 lacp workp 2* *oder* *switch(config)#aggregator group 2 1,4,3 lacp workp 3*
`aggregator group [GroupID] [Port-list] nolacp`	*G*	Weist eine statische Trunk-gruppe zu. [***GROUPID] :***1 - 3 [***PORT-LIST***]: Liste von Member Ports. Dieser Wert kann eine Bandbreite von Ports (ex. 1 - 4) oder eine durch Kommas getrennte Portliste sein (ex. 2, 3, 6).	*switch(config)#aggregator group 1 2-4 nolacp* *oder* *switch(config)#aggregator group 1 3,1,2 nolacp*

Befehl	Stufe	Beschreibung	Beispiel
`show aggregator`	*P*	Zeigt Informationen zu einer Trunk-Gruppe an.	*switch#show aggregator 1* *oder* *switch#show aggregator 2* *oder* *switch#show aggregator 3*
`no aggregator lacp [GroupID]`	*G*	Deaktiviert die LACP-Funktion der Trunk-Gruppe.	*switch(config)#no aggreator lacp 1*
`no aggregator group [GroupID]`	*G*	Entfernt eine Trunk-Gruppe.	*switch(config)#no aggreator group 2*

4.8 VLAN-Befehle

Befehl	Stufe	Beschreibung	Beispiel
`vlan database`	*P*	Mit diesem Befehl gelangen Sie in den VLAN-Konfigurationsmodus.	*switch#vlan database*
`Vlanmode [portbase| 802.1q | gvrp]`	*V*	Setzt den Switch in den VLAN-Modus.	*switch(vlan)#vlanmode portbase* *oder* *switch(vlan)#vlanmode 802.1q* *oder* *switch(vlan)#vlanmode gvrp*
`no vlan`	*V*	Kein VLAN	*Switch(vlan)#no vlan*
Port-basierte VLAN-Konfiguration			

Befehl	Stufe	Beschreibung	Beispiel
`vlan port-based grpname [Group Name] grpid [GroupID] port [PortNumbers]`	*V*	Fügt ein neues, Port-basiertes VLAN hinzu.	*switch(vlan)#vlan port-based grp-name test grpid 2 port 2-4 oder switch(vlan)#vlan port-based grp-name test grpid 2 port 2,3,4*
`show vlan [GroupID] oder show vlan`	*V*	Zeigt VLAN-Informationen an.	*switch(vlan)#show vlan 23*
`no vlan group[GroupID]`	*V*	Löscht das mit "ID" bezeichnete VLAN.	*switch(vlan)#no vlan group 2*
IEEE 802.1Q VLAN			
`vlan 8021q name [GroupName] vid [VID]`	*V*	Ändert den Namen der VLAN-Gruppe. Wenn die Gruppe nicht existiert, kann dieser Befehl nicht angewendet werden.	*switch(vlan)#vlan 8021q name test vid 22*
`vlan 8021q port [PortNumber] access-link untag [UntaggedVID]`	*V*	Weist dem VLAN einen Port-basierten Access Link zu. Wenn der Port zu einer Trunk-Gruppe gehört, kann dieser Befehl nicht angewendet werden.	*switch(vlan)#vlan 8021q port 3 access-link untag 33*
`vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]`	*V*	Weist dem VLAN einen Port-basierten Trunk Link zu. Wenn der Port zu einer Trunk-Gruppe gehört, kann dieser Befehl nicht angewendet werden.	*switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 oder switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20*

Befehl	Stufe	Beschreibung	Beispiel
`vlan 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]`	*V*	Weist dem VLAN einen Port-basierten, hybriden Link zu. Wenn der Port zu einer Trunk-Gruppe gehört, kann dieser Befehl nicht angewendet werden.	*switch(vlan)#vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 oder switch(vlan)#vlan 8021q port 3 hybrid-link untag 5 tag 6-8*
`vlan 8021q trunk [PortNumber] access-link untag [UntaggedVID]`	*V*	Weist dem VLAN einen Access Link nach Trunk-Gruppe zu.	*switch(vlan)#vlan 8021q trunk 3 access-link untag 33*
`vlan 8021q trunk [PortNumber] trunk-link tag [TaggedVID List]`	*V*	Weist dem VLAN einen Trunk Link nach Trunk-Gruppe zu.	*switch(vlan)#vlan 8021q trunk 3 trunk-link tag 2,3,6,99 oder switch(vlan)#vlan 8021q trunk 3 trunk-link tag 3-20*
`vlan 8021q trunk [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]`	*V*	Weist dem VLAN einen hybriden Link nach Trunk-Gruppe zu.	*switch(vlan)#vlan 8021q trunk 3 hybrid-link untag 4 tag 3,6,8 oder switch(vlan)#vlan 8021q trunk 3 hybrid-link untag 5 tag 6-8*
`show vlan [GroupID] oder show vlan`	*V*	Zeigt VLAN-Informationen an.	*switch(vlan)#show vlan 23*
`no vlan group [GroupID`	*V*	Löscht das mit "ID" bezeichnete VLAN.	*switch(vlan)#no vlan group 2*

4.9 Spanning-Tree-Befehle

Befehl	Stufe	Beschreibung	Beispiel
`spanning-tree enable`	*G*	Aktiviert Spanning Tree.	*switch(config)#spanning-tree enable*
`spanning-tree priority [0-61440]`	*G*	Konfiguriert die Spanning-Tree-Prioritätsparameter.	*switch(config)#spanning-tree priority 32767*
`spanning-tree max-age [seconds]`	*G*	Verwenden Sie den globalen Konfigurationsbefehl für Spanning Tree mit der maximalen Lebensdauer, um die Zeitabstände zu ändern, zwischen denen der Spanning Tree Meldungen vom Root Switch empfängt. Wenn der Switch innerhalb dieses Zeitraums keine BPDU-Meldung (Bridge Protocol Data Unit) vom Root Switch erhält, berechnet er die Topologie des Spanning Tree Protokolls (STP) neu.	*switch(config)#spanning-tree max-age 15*
spanning-tree hello-time [seconds]	*G*	Verwenden Sie den globalen Hello-Time-Konfigurationsbefehl für Spanning Tree, um die Zeitabstände zwischen Hello-BPDUs (Bridge Protocol Data Units) festzulegen.	*switch(config)#spanning-tree hello-time 3*

Befehl	Stufe	Beschreibung	Beispiel
`spanning-tree forward-time [seconds]`	*G*	Verwenden Sie den globalen Konfigurationsbefehl zur Weiterleitungszeit für Spanning Tree, um die Weiterleitungszeit für den angegebenen Spanning-Tree festzulegen. Die Weiterleitungszeit bestimmt, wie lange jeder Listening- und Learning-Zustand dauert, bevor der Port mit der Weiterleitung beginnt.	*switch(config)#spanning-tree forward-time 20*
`stp-path-cost [1-200000000]`	*I*	Verwenden Sie den Spanning Tree Cost Interface Konfigurationsbefehl, um die Pfadkosten für Berechnungen nach dem Spanning Tree Protokoll (STP) festzulegen. Wird eine Schleife gebildet, dann berücksichtig Spanning Tree die Pfadkosten, die bei der Auswahl einer Schnittstelle auftreten, die in den Weiterleitungsstatus geschaltet wird.	*switch(config)#interface fastEthernet 2* *switch(config-if)#stp-path-cost 20*
`stp-path-priority [Port Priority]`	*I*	Verwenden Sie den Schnittstellenkonfigurations-befehl für Portpriorität für Spanning Tree. Damit wird die Portpriorität festgelegt, die verwendet wird, um die Bridge ID zu bilden und die Root Bridge zu bestimmen.	*switch(config)#interface fastEthernet 2* *switch(config-if)#stp-path-priority 128*

Befehl	Stufe	Beschreibung	Beispiel
stp-admin-p2p [Auto|True|False]	*I*	Konfiguration der Schnittstelle als P2P-Port	*switch(config)#interface fastEthernet 2switch(config-if)#stp-admin-p2p Auto*
`stp-admin-edge [True|False]`	*I*	Konfiguration der Schnittstelle als Edge Port	*switch(config)#interface fastEthernet 2switch(config-if)#stp-admin-edge True*
`stp-admin-non-stp [True|False]`	*I*	Deaktivierung des STP auf dieser Schnittstelle durch den Administrator	*switch(config)#interface fastEthernet 2 switch(config-if)#stp-admin-non-stp False*
`show spanning-tree`	*E*	Zeigt eine Zusammenfassung der Spanning-Tree-Zustände.	*switch>show spanning-tree*
`no spanning-tree`	*G*	Deaktiviert Spanning Tree.	*switch(config)#no spanning-tree*

4.10 QoS-Befehle

Befehl	Stufe	Beschreibung	Beispiel
`qos policy [weighted-fair| strict]`	*G*	Legt QoS-Policy fest.	*switch(config)#qos policy weighted-fair*
`qos prioritytype [port-based|cos-only|tos -only|cos-first|tos-first]`	*G*	Legt QoS-Prioritätstyp fest.	*switch(config)#qos prioritytype*

Befehl	Stufe	Beschreibung	Beispiel
`qos priority portbased [Port] [lowest|low|middle|high]`	*G*	Konfiguriert Port-basierte Priorität.	*switch(config)#qos priority portbased 1 low*
`qos priority cos [Priority][lowest|low|middle|high]`	*G*	Konfiguriert CoS-Priorität.	*switch(config)#qos priority cos 0 middle*
`qos priority tos [Priority][lowest|low|middle|high]`	*G*	Konfiguriert ToS-Priorität.	*switch(config)#qos priority tos 3 high*
`show qos`	*P*	Zeigt Informationen zur QoS-Konfiguration an.	*Switch#show qos*
`no qos`	*G*	Deaktiviert die QoS-Funktion.	*switch(config)#no qos*

4.11 IGMP-Befehle

Befehl	Stufe	Beschreibung	Beispiel
`igmp enable`	*G*	Aktiviert die IGMP-Snooping-Funktion.	*switch(config)#igmp enable*
`Igmp-query auto`	*G*	Setzt IGMP-Abfrage auf Auto-Modus.	*switch(config)#Igmp-query auto*
`Igmp-query force`	*G*	Setzt IGMP-Abfrage auf erzwungenen Modus (forced mode).	*switch(config)#Igmp-query force*
`show igmp configuration`	*P*	Zeigt Details einer IGMP-Konfiguration an.	*switch#show igmp configuration*

Befehl	Stufe	Beschreibung	Beispiel
`show igmp multi`	*P*	Zeigt Details eines IGMP-Snooping-Eintrags an.	*switch#show igmp multi*
`no igmp`	*G*	Deaktiviert die IGMP-Snooping-Funktion.	*switch(config)#no igmp*
`no igmp-query`	*G*	Deaktiviert IGMP-Abfrage.	*switch#no igmp-query*

4.12 MAC- / Filtertabellenbefehle

Befehl	Stufe	Beschreibung	Beispiel
`mac-address-table static hwaddr [MAC]`	*I*	Konfiguriert die MAC-Adresstabelle der Schnittstelle (statisch).	*switch(config)#interface fastEthernet 2switch(config-if)#mac-address-table static hwaddr 000012345678*
`mac-address-table filter hwaddr [MAC]`	*G*	Konfiguriert die MAC-Adresstabelle (Filter)	*switch(config)#mac-address-table filter hwaddr 000012348678*
`show mac-address-table`	*P*	Zeigt alle MAC-Adresstabellen an.	*switch#show mac-address-table*
`show mac-address-table static`	*P*	Zeigt eine statische MAC-Adresstabelle an.	*switch#show mac-address-table static*
`show mac-address-table filter`	*P*	Zeigt einen Filter für eine MAC-Adresstabelle.	*switch#show mac-address-table filter*
`no mac-address-table static hwaddr [MAC]`	*I*	Entfernt einen Eintrag in der MAC-Adresstabelle der Schnittstelle (statisch).	*switch(config)#interface fastEthernet 2switch(config-if)#no mac-address-table static hwaddr 000012345678*
`no mac-address-table filter hwaddr [MAC]`	*G*	Entfernt einen Eintrag aus der MAC-Adresstabelle (Filter).	*switch(config)#no mac-address-table filter hwaddr 000012348678*

Befehl	Stufe	Beschreibung	Beispiel
`no mac-address-table`	*G*	Entfernt einen dynamischen Eintrag aus der MAC-Adresstabelle.	*switch(config)#no mac-address-table*

4.13 SNMP-Befehle

Befehl	Stufe	Beschreibung	Beispiel
`snmp system-name [System Name]`	*G*	Legt den Systemnamen des SNMP-Agenten fest.	*switch(config)#snmp system-name l2switch*
`snmp system-location [System Location]`	*G*	Legt den Ort des SNMP-Agenten fest.	*switch(config)#snmp system-location lab*
`snmp system-contact [System Contact]`	*G*	Legt den Kontakt des SNMP-Agenten fest.	*switch(config)#snmp system-contact where*
`snmp agent-mode [v1v2c|v3|v1v2cv3]`	*G*	Wählt den Agentenmodus für SNMP aus.	*switch(config)#snmp agent-mode v1v2cv3*
`snmp community-strings [Community]right[RO/RW]`	*G*	Fügt einen SNMP Community String hinzu.	*switch(config)#snmp community-strings public right rw*
`snmp-server host [IP address] community [Community-string] trap-version [v1|v2c]`	*G*	Konfiguriert Hostinformationen und den Community String für den SNMP-Server.	*switch(config)#snmp-server host 192.168.1.50 community public trap-version v1(remove)Switch(config)#no snmp-server host192.168.1.50*
`snmpv3 context-name [Context Name ]`	*G*	Konfiguriert den Kontextnamen.	*switch(config)#snmpv3 context-name Test*

Befehl	Stufe	Beschreibung	Beispiel
`snmpv3 user [User Name] group [Group Name] password [Authentication Password] [Privacy Password]`	*G*	Konfiguriert das Benutzerprofil für den SNMPv3-Agenten. Es wurde möglicherweise kein Privacy Password vergeben.	*switch(config)#snmpv3 user test01 group G1 password AuthPW PrivPW*
`snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv|AuthNoPriv|AuthPriv] match-rule [Exact|Prifix] views [Read View Name] [Write View Name] [Notify View Name]`	*G*	Konfiguriert die Zugangstabelle des SNMPv3-Agenten.	*switch(config)#snmpv3 access context-name Test group G1 security-level AuthPrivmatch-rule Exact views V1 V1 V1*
`snmpv3 mibview view [View Name] type [Excluded|Included] sub-oid [OID]`	*G*	Konfiguriert die mibview - Tabelle des SNMPv3-Agenten.	*switch(config)#snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1*
`show snmp`	*P*	Zeigt die SNMP-Konfiguration.	*switch#show snmp*
`no snmp community-strings [Community]`	*G*	Entfernt die angegebene Community.	*switch(config)#no snmp community-strings public*

Befehl	Stufe	Beschreibung	Beispiel
`no snmp-server host [Host-address]`	*G*	Entfernt den SNMP Server Host.	*switch(config)#no snmp-server 192.168.1.50*
`no snmpv3 user [User Name]`	*G*	Entfernt den angegebenen Benutzer des SNMPv3-Agenten.	*switch(config)#no snmpv3 user Test*
`no snmpv3 access context-name [Context Name] group [Group Name] security-level [NoAuthNoPriv|AuthNoPriv|AuthPriv] match-rule [Exact|Prifix] views [Read View Name] [Write View Name] [Notify View Name]`	*G*	Entfernt die angegebene Zugangstabelle des SNMPv3-Agenten.	*switch(config)#no snmpv3 access context-name Test group G1 security-level AuthPriv match-rule Exact views V1 V1 V1*
`no snmpv3 mibview view [View Name] type [Excluded|Included] sub-oid [OID]`	*G*	Entfernt die angegebene mibview-Tabelle des SNMPv3-Agenten.	*switch(config)#no snmpv3 mibview view V1 type Excluded sub-oid 1.3.6.1*

4.14 Port-Mirroring-Befehle

Befehl	Stufe	Beschreibung	Beispiel
`monitor rx`	*G*	Legt den RX-Zielport der Überwachungsfunktion fest.	*switch(config)#monitor rx*
`monitor tx`	*G*	Legt den TX-Zielport der Überwachungsfunktion fest.	*switch(config)#monitor tx*
`show monitor`	*P*	Zeigt Informationen zur Portüberwachung an.	*switch#show monitor*
`monitor [RX|TX|Both]`	*I*	Konfiguriert den Quellport der Überwachungsfunktion.	*switch(config)#interface fastEthernet 2* *switch(config-if)#monitor RX*
`show monitor`	*I*	Zeigt Informationen zur Portüberwachung an.	*switch(config)#interface fastEthernet 2* *switch(config-if)#show monitor*
`no monitor`	*I*	Deaktiviert den Quellport der Überwachungsfunktion.	*switch(config)#interface fastEthernet 2* *switch(config-if)#no monitor*

4.15 802.1x-Befehle

Befehl	Stufe	Beschreibung	Beispiel
`8021x enable`	*G*	Verwenden Sie den globalen 802.1x Konfigurationsbefehl, um 802.1x-Protokolle zu aktivieren.	*switch(config)# 8021x enable*

Befehl	Stufe	Beschreibung	Beispiel
`8021x system radiusip [IP address]`	*G*	Verwenden Sie den globalen Konfigurationsbefehl 802.1x System Radius IP, um die IP-Adresse des Radius Servers zu ändern.	*switch(config)# 8021x system radiusip 192.168.1.1*
`8021x system serverport [port ID]`	*G*	Verwenden Sie den globalen Konfigurationsbefehl für den Server Port für 802.1x, um den Radius Server Port zu ändern.	*switch(config)# 8021x system serverport 1815*
`8021x system accountport [port ID]`	*G*	Verwenden Sie den globalen Konfigurationsbefehl für den Accounting Port für 802.1x, um den Accounting Port zu ändern.	*switch(config)# 8021x system accountport 1816*
`8021x system sharekey [ID]`	*G*	Verwenden Sie den globalen Konfigurationsbefehl für den Shared Key für 802.1x, um den Wert für den Shared Key zu ändern.	*switch(config)# 8021x system sharekey 123456*
`8021x system nasid [words]`	*G*	Verwenden Sie den globalen Konfigurationsbefehl für die NAS ID für 802.1x, um die NAS ID zu ändern.	*switch(config)# 8021x system nasid test1*
`8021x misc quietperiod [sec.]`	*G*	Verwenden Sie den globalen Konfigurationsbefehl für die Misc Quiet Periods (verschiedene Ruhephasen), um den Wert für die Quiet Periods (Ruhephasen) des Switch festzulegen.	*switch(config)# 8021x misc quietperiod 10*

Befehl	Stufe	Beschreibung	Beispiel
`8021x misc txperiod [sec.]`	*G*	Verwenden Sie den globalen Konfigurationsbefehl für die Misc TX Period für 802.1x, um die TX Period festzulegen, die den Zeitraum bis zur Weitersendung von Authentifizierungsinformation definiert.	*switch(config)# 8021x misc txperiod 5*
`8021x misc supportimeout [sec.]`	*G*	Verwenden Sie den globalen Konfigurationsbefehl für den Misc Supplicant Timeout für 802.1x, um den Supplicant Timeout festzulegen.	*switch(config)# 8021x misc supportimeout 20*
`8021x misc servertimeout [sec.]`	*G*	Verwenden Sie den globalen Konfigurationsbefehl für den Misc Server Timeout für 802.1x, um den Server Timeout festzulegen.	*switch(config)#8021x misc servertimeout 20*
`8021x misc maxrequest [number]`	*G*	Verwenden Sie den globalen Konfigurationsbefehl für die Misc MAX Request für 802.1x, um die MAX Requests festzulegen.	*switch(config)# 8021x misc maxrequest 3*
`8021x misc reauthperiod [sec.]`	*G*	Verwenden Sie den globalen Konfigurationsbefehl für die Misc Reauthentication Period für 802.1x, um die Reauthentication Period festzulegen.	*switch(config)# 8021x misc reauthperiod 3000*

Befehl	Stufe	Beschreibung	Beispiel
`8021x portstate [disable | reject | accept | authorize]`	*I*	Verwenden Sie den Schnittstellenkonfigurations-befehl 802.1x Port State, um den Zustand des ausgewählten Ports festzulegen.	*switch(config)#interface fastethernet 3 switch(config-if)#8021x port-state accept*
`show 8021x`	*E*	Zeigt eine Zusammenfassung der Eigenschaften von 802.1 und der Portzustände an.	*switch>show 8021x*
`no 8021x`	*G*	Deaktiviert die 802.1x-Funktion.	*switch(config)#no 8021x*

4.16 TFTP-Befehle

Befehl	Stufe	Beschreibung	Beispiel
`backup flash:backup_cfg`	*G*	Speichert die Konfiguration unter TFTP. Die IP-Adresse des TFTP-Servers und der Dateiname müssen festgelegt werden.	*switch(config)#backup flash:backup_cfg*
`restore flash:restore_cfg`	*G*	Erhält die Konfiguration vom TFTP-Server. Die IP-Adresse des TFTP-Servers und der Dateiname müssen festgelegt werden.	*switch(config)#restore flash:restore_cfg*

Befehl	Stufe	Beschreibung	Beispiel
`upgrade flash:upgrade_fw`	*G*	Upgrade der Firmware über TFTP. Die IP-Adresse des TFTP-Servers und der Dateiname müssen festgelegt werden.	*switch(config)#upgrade lash:upgrade_fw*

4.17 System Log-, SMTP- und Ereignisbefehle

Befehl	Stufe	Beschreibung	Beispiel
`systemlog ip [IP address]`	*G*	Legt die IP-Adresse des System Log Servers fest.	*switch(config)# systemlog ip 192.168.1.100*
`systemlog mode [client|server|both]`	*G*	Spezifiziert den Protokoll-Modus.	*switch(config)# systemlog mode both*
`show systemlog`	*E*	Zeigt das Systemprotokoll an.	*Switch>show systemlog*
`show systemlog`	*P*	Zeigt den System Log Client und Serverinformationen an.	*switch#show systemlog*
`no systemlog`	*G*	Deaktiviert die Systemprotokoll-Funktion.	*switch(config)#no systemlog*
`smtp enable`	*G*	Aktiviert die SMTP-Funktion.	*switch(config)#smtp enable*
`smtp serverip [IP address]`	*G*	Konfiguriert die SMTP Server ID.	*switch(config)#smtp serverip 192.168.1.5*
`smtp authentication`	*G*	Aktiviert die SMTP-Authentifizierung.	*switch(config)#smtp authentication*

Befehl	Stufe	Beschreibung	Beispiel
`smtp account [account]`	*G*	Konfiguriert den Authentifizierungs-Account.	*switch(config)#smtp account User*
`smtp password [password]`	*G*	Konfiguriert das Authentifizierungs-Passwort.	*switch(config)#smtp password*
`smtp rcptemail [Index] [Email address]`	*G*	Konfiguriert die E-Mail-adresse des Empfängers.	*switch(config)#smtp rcptemail 1* Alert@test.com
`show smtp`	*P*	Zeigt Informationen zur SMTP an.	*switch#show smtp*
`no smtp`	*G*	Deaktiviert die SMTP-Funktion.	*switch(config)#no smtp*
`event device-cold-start [Systemlog|SMTP|Both]`	*G*	Legt die Ereignisart für Kaltstart fest.	*switch(config)#event device-cold-start both*
`event authentication-failure [Systemlog|SMTP|Both]`	*G*	Legt die Ereignisart für fehlgeschlagene Authentifizierung fest.	*switch(config)#event authentication-failure both*
`event X-ring-topology-change[Systemlog|SMTP|Both]`	*G*	Legt Ereignisart für geänderte X-Ring-Topologie fest.	*switch(config)#event X-ring-topology-change both*
`event systemlog [Link-UP|Link-Down|Both]`	*I*	Legt Portereignis für Systemprotokoll fest.	*switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both*
`event smtp [Link-UP|Link-Down|Both]`	*I*	Legt Portereignis für SMTP fest.	*switch(config)#interface fastethernet 3switch(config-if)#event smtp both*

Befehl	Stufe	Beschreibung	Beispiel
`show event`	*P*	Zeigt eine Auswahl von Ereignissen.	*switch#show event*
`no event device-cold-start`	*G*	Deaktiviert die Ereignisart für Kaltstart.	*switch(config)#no event device-cold-start*
`no event authentication-failure`	*G*	Deaktiviert die Ereignisart für fehlgeschlagene Authentifizierung.	*switch(config)#no event authentication-failure*
`no event X-ring-topology-change`	*G*	Deaktiviert die Ereignisart für geänderte X-Ring-Topologie.	*switch(config)#no event X-ring-topology-change*
`no event systemlog`	*I*	Deaktiviert Portereignis für Systemprotokoll.	*switch(config)#interface fastethernet 3* *switch(config-if)#no event systemlog*
`no event smpt`	*I*	Deaktiviert Portereignis für SMTP.	*switch(config)#interface fastethernet 3* *switch(config-if)#no event smtp*
`show systemlog`	*P*	Zeigt den System Log Client und Serverinformationen an.	*switch#show systemlog*

4.18 SNTP-Befehle

Befehl	Stufe	Beschreibung	Beispiel
`sntp enable`	*G*	Aktiviert die SNTP-Funktion.	*switch(config)#sntp enable*

Befehl	Stufe	Beschreibung	Beispiel
`sntp daylight`	*G*	Aktiviert das Zeitfenster, in dem tagsüber gesichert wird. Wenn die SNTP-Funktion deaktiviert wurde, kann dieser Befehl nicht angewendet werden.	*switch(config)#sntp daylight*
`sntp daylight-period [Start time] [End time]`	*G*	Legt das Zeitfenster fest, in dem tagsüber gesichert wird. Wenn die SNTP-Funktion deaktiviert wurde, kann dieser Befehl nicht angewendet werden. Format des Parameters: [yyyymmdd-hh:mm]	*switch(config)#sntp daylight-period 20060101-01:01 20060202-01-01*
`sntp daylight-offset [Minute]`	*G*	Legt den Versatz des Zeitfensters fest, in dem tagsüber gesichert wird. Wenn die SNTP-Funktion deaktiviert wurde, kann dieser Befehl nicht angewendet werden.	*switch(config)#sntp daylight-offset 3*
`sntp ip [IP]`	*G*	Legt die IP-Adresse des SNTP-Servers fest. Wenn die SNTP-Funktion deaktiviert wurde, kann dieser Befehl nicht angewendet werden.	*switch(config)#sntp ip 192.169.1.1*
`sntp timezone [Timezone]`	*G*	Legt den Zeitzonen-Index fest. Verwenden Sie den Befehlt "show sntp timzezone", um weitere Informationen zur Indexnummer zu erhalten.	*switch(config)#sntp timezone 22*
`show sntp`	*P*	Zeigt SNTP-Informationen an.	*switch#show sntp*

Befehl	Stufe	Beschreibung	Beispiel
`show sntp timezone`	*P*	Zeigt die Indexnummer der Zeitzonenliste an.	*switch#show sntp timezone*
`no sntp`	*G*	Deaktiviert die SNTP-Funktion.	*switch(config)#no sntp*
`no sntp daylight`	*G*	Deaktiviert Sichern tags-über.	*switch(config)#no sntp daylight*

4.19 X-Ring-Befehle

Befehl	Stufe	Beschreibung	Beispiel
`Xring enable`	*G*	Aktiviert den X-Ring.	*switch(config)#Xring enable*
`Xring master`	*G*	Aktiviert den Ring Master.	*switch(config)#Xring master*
`X-Ring couplering`	*G*	Aktiviert den Koppelring.	*switch(config)#Xring couplering*
`X-Ring Dual Homing`	*G*	Aktiviert Dual Homing	*switch(config)#Xring dualho-ming*
`Xring ringport [1st Ring Port] [2nd Ring Port]`	*G*	Konfiguriert 1./2. Ring Port.	*switch(config)#Xring ringport 7 8*
`Xring couplingport [Coupling Port]`	*G*	Konfiguriert den Koppel-port.	*switch(config)#Xring coupling-port 1*
`Xring controlport [Control Port]`	*G*	Konfiguriert den Steuer-port.	*switch(config)#Xring controlport 2*
`Xring homingport [Dual Homing Port]`	*G*	Konfiguriert den Dual Homing Port.	*switch(config)#Xring homingport 3*
`show Xring`	*P*	Zeigt Informationen zum X-Ring an.	*switch#show Xring*

Befehl	Stufe	Beschreibung	Beispiel
`no Xring`	*G*	Deaktiviert den X-Ring.	*switch(config)#no X ring*
`no Xring master`	*G*	Deaktiviert den Ring Master.	*switch(config)# no Xring master*
`no Xring couplering`	*G*	Deaktiviert den Koppelring.	*switch(config)# no Xring couplering*
`no Xring dualhoming`	*G*	Deaktiviert Dual Homing	*switch(config)# no Xring dualhoming*

5 Web-basiertes Management

Dieser Abschnitt führt Sie in die Konfiguration und die Funktionen des Web-basierten Managements ein.

5.1 Web-basiertes Management

Die web-basierte Management-Funktion ermöglicht es dem Benutzer, den Switch von jeder Stelle des Netzwerks aus über einen unterstützen Standard-Browser zu managen.

Das Web-basierte Management unterstützt den Internet Explorer 6.0 und höhere Versionen. Die Anwendung mit Java Applets benötigt weniger Bandbreite, erhöht die Zugriffsgeschwindigkeit und bietet dem Benutzer einen Bildschirm, der einfach zu überschauen ist.

5.2 Vorbereitung für Web Management

Bevor Sie das Web Management nutzen, können Sie die Konsole zum Login am Switch verwenden. Prüfen Sie dabei die Default-IP-Adresse des Switch. Im Kapitel Konsolenmanagement finden Sie Informationen zum Login über die Konsole. Wenn Sie die IP-Adresse zum ersten Mal ändern müssen, können Sie die Konsole zum Ändern benutzen. Die Standardeinstellungen sind wie folgt:

IP-ADRESSE: *192.168.0.248*

SUBNETZMASKE: *255.255.255.0*

DEFAULT GATEWAY: *keiner*

BENUTZERNAME: admin ***PASSWORT:*** *funkwerk*

5.3 System Login

- Starten Sie den Internet Explorer.
- Geben Sie http:// und die IP-Adresse des Switch ein und drücken Sie dann die **Enter**-Taste.
- Das Login-Menü erscheint.
- Geben Sie den Benutzernamen und das Password ein. Der Standard-Benutzername ist *admin* und das Standard-Passwort ist *funkwerk*.
- Klicken Sie auf **Enter** oder **OK**. Die Homepage der Applikation Web-basiertes Management erscheint.

Abbildung 5-1: Oberfläche Web-basiertes Management

5.4 Systeminformationen

Hier können Sie den Systemnamen und das Verzeichnis zuweisen und Systeminformationen einsehen.

- ***System Name:*** Legen Sie den Systemnamen des Switch fest (maximale Länge: 64 Zeichen).
- ***System Location:*** Definieren Sie den physikalischen Ort, an dem der Switch platziert ist (maximale Länge: 64 Zeichen).
- ***System Description:*** Zeigt die Beschreibung des Switch an (im Read-only-Modus, nicht veränderbar).
- ***Firmware Version:*** Gibt die Firmware-Version des Switch an.
- ***Kernel Version:*** Gibt die Kernel-Software-Version an.
- ***Hardware version:*** Gibt die Hardware-Version des Switch an.
- ***MAC Address:*** Gibt die eindeutige Hardware-Adresse an, die standardmäßig vom Hersteller vergeben wird.
- Klicken Sie auf **Apply**.

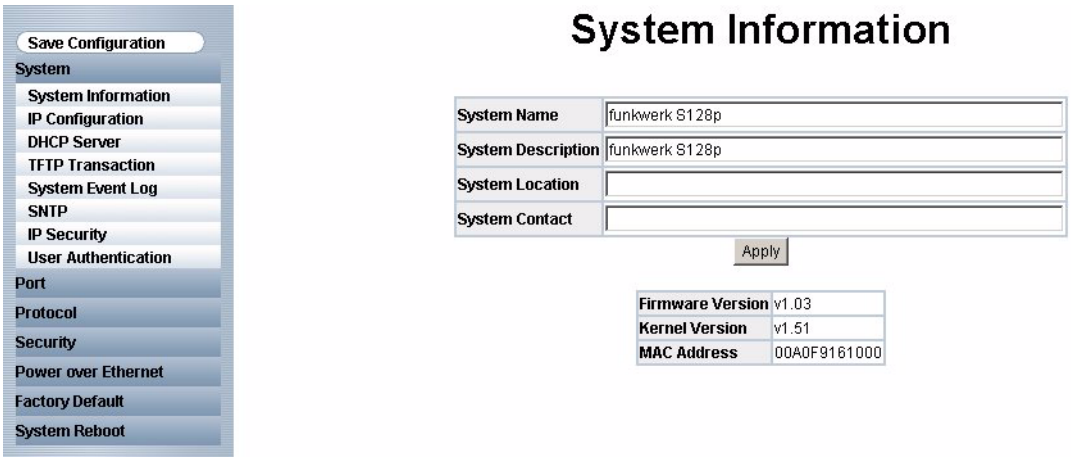


Abbildung 5-2: Oberfläche zu Systeminformationen

5.5 IP-Konfiguration

Der Benutzer kann die IP-Einstellungen und die DHCP-Client-Funktion konfigurieren.

- ***DHCP:*** Aktiviert bzw. deaktiviert die DHCP-Client-Funktion.
- ***IP ADDRESS:*** Weist dem Switch eine IP-Adresse zu. Die Standard-IP-Adresse ist 192.168.248
- ***SUBNET MASK:*** Weist dem Switch eine IP-Subnetzmaske zu.
- ***GATEWAY:*** Weist dem Switch einen Gateway zu. Die Standardwert ist 0.0.0.0 (kein Gateway).
- ***DNS1:*** Abkürzung für Domain Name Server. DNS1 ist der primäre Domain Name Server, der standardmäßig genutzt wird.
- ***DNS2:*** Der sekundäre Domain Name Server, also das Backup für DNS1. Wenn DNS1 ausfällt, übernimmt DNS2 sofort dessen Funktion.
- Klicken Sie auf **Apply**.
- Starten Sie den Switch neu, nachdem Sie die IP-Adresse zurückgesetzt haben.

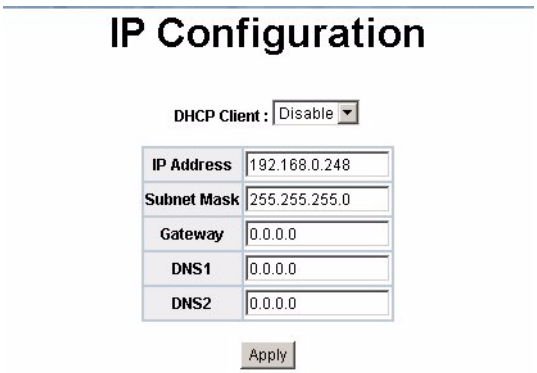


Abbildung 5-3: Oberfläche zur IP-Konfiguration

5.6 DHCP-Konfiguration

DHCP ist eine Abkürzung für Dynamic Host Configuration Protocol. Das ist ein Protokoll, mit dem Geräten in einem Netzwerk dynamische IP-Adressen zugewiesen werden. Bei dynamischer Adressierung kann einem Gerät immer wieder eine neue IP-Adresse zugewiesen werden, wenn es sich wieder am Netzwerk anmeldet. Bei einigen Systemen kann sich die IP-Adresse eines Geräts sogar ändern, während es noch mit dem Netzwerk verbunden ist. DHCP unterstützt also einen Mix aus statischen und dynamischen IP-Adressen. Die dynamische Adressierung vereinfacht die Netzwerkadministration, da in diesem Fall die Software die IP-Adressen verwaltet und dem Administrator die Durchführung dieser Aufgabe abnimmt. Das bedeutet, ein weiterer Rechner kann dem Netzwerk hinzugefügt werden, ohne dass man dabei umständlich manuell eine eindeutige IP-Adresse neu vergeben muss.

5.6.1 Konfiguration des DHCP-Servers

Das System stellt die Funktion des DHCP-Servers zur Verfügung. Durch Aktivierung der DHCP-Server-Funktion wird der Switch zum DHCP-Server.

- ***DHCP Server:*** Aktiviert bzw. deaktiviert die DHCP-Server-Funktion. Enable – der Switch wird zum DHCP-Server in Ihrem lokalen Netzwerk.
- ***Low IP Address:*** Dynamischer IP-Adressbereich. Eine niedrige IP-Adresse steht am Anfang des dynamischen IP-Adressbereichs. Beispiel: der dynamische IP-Adressbereich erstreckt sich von 192.168.1.100 bis 192.168.1.200. Die niedrigste IP-Adresse ist hier 192.168.1.100.
- ***High IP Address:*** Dynamischer IP-Adressbereich. Eine hohe IP-Adresse steht am Ende des dynamischen IP-Adressbereichs. Beispiel: der dynamische IP-Adressbereich erstreckt sich von 192.168.1.100 bis 192.168.1.200. Die höchste IP-Adresse ist hier 192.168.1.200.
- ***Subnet Mask:*** Der dynamische IP-Adressbereich der Subnetzmaske
- ***Gateway:*** Der Gateway Ihres Netzwerks
- ***DNS:*** Die IP-Adresse des Domain Name Servers in Ihrem Netzwerk

- ***LEASE TIME (SEC):*** Das ist die Zeitspanne, nach der das System die dynamische IP-Adresse zurücksetzt und neu zuweist. Damit wird verhindert, dass die dynamische IP-Adresse zu lange belegt wird oder dass der Server nicht erfährt, dass eine dynamische IP-Adresse nicht genutzt wird.

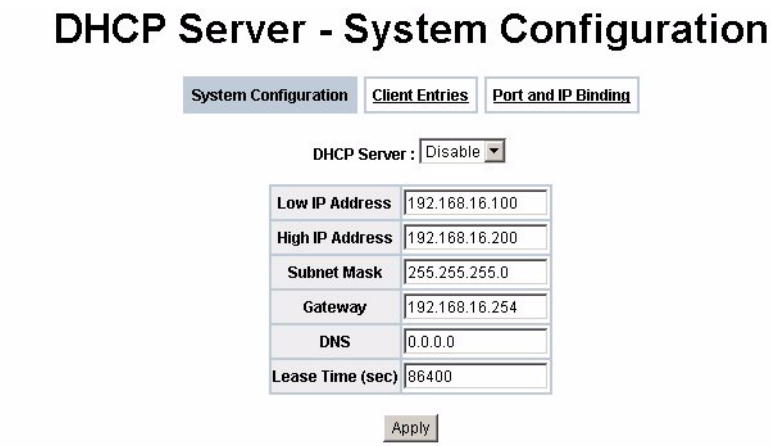


Abbildung 5-4: Oberfläche zur Konfiguration des DHCP-Servers

5.6.2 Einträge des DHCP Clients

Wurde die DHCP-Server-Funktion deaktiviert, dann speichert das System die Informationen zum DHCP-Client hier ab und zeigt sie an.

Abbildung 5-5: Oberfläche zu Einträgen des DHCP Clients

5.6.3 Port und IP Binding

Weisen Sie die dynamische IP-Adresse dem Port zu. Wenn das Gerät an den Port angeschlossen wird und die Zuweisung einer IP-Adresse anfordert, wird das System ihm die IP-Adresse zuweisen, die vorher für das angeschlossene Gerät vergeben wurde.

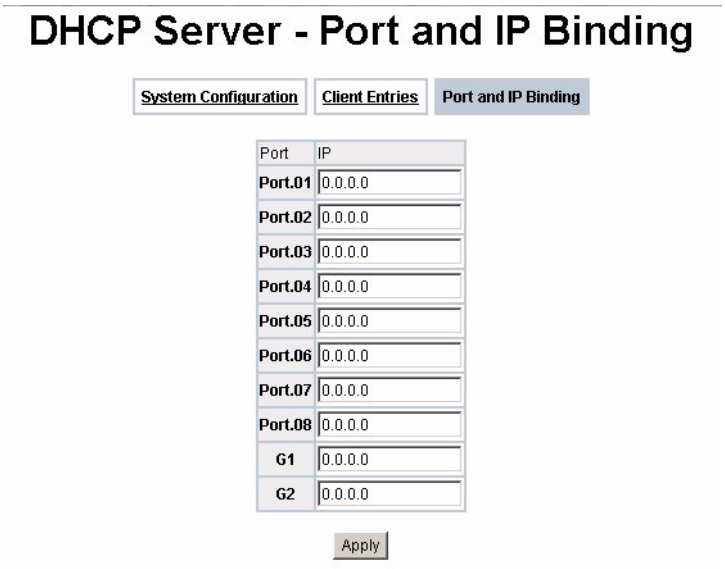


Abbildung 5-6: Oberfläche zu Port und IP Binding

5.7 Update Firmware

Dieser Menüpunkt stellt die Funktionen zur Verfügung, die benötigt werden, um die Switch Firmware upzudaten. Bevor Sie das Update durchführen, stellen Sie sicher, dass der TFTP-Server in Betrieb und das Firmware Image auf dem TFTP-Server verfügbar ist.

- ***TFTP SERVER IP ADDRESS:*** Geben Sie die IP-Adresse des TFTP-Servers ein.
- ***FIRMWARE FILE NAME:*** Name des Firmware Image
- Klicken Sie auf **Apply**.

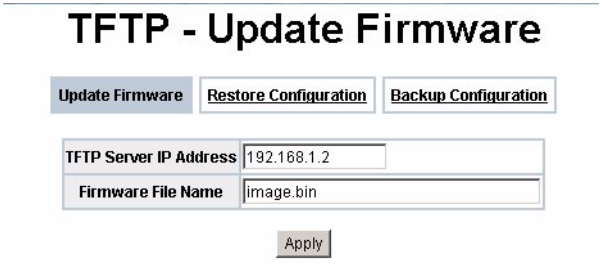


Abbildung 5-7: Oberfläche zum Update der Firmware

5.8 Konfiguration wiederherstellen

Unter diesem Menüpunkt stellen Sie den EEPROM-Wert vom TFTP-Server aus wieder her.

- ***TFTP SERVER IP ADDRESS:*** Geben Sie die IP-Adresse des TFTP-Servers ein.
- ***RESTORE FILE NAME:*** Geben Sie den Namen der Konfigurationsdatei ein, die Sie wiederherstellen wollen.
- Klicken Sie auf **Apply**.

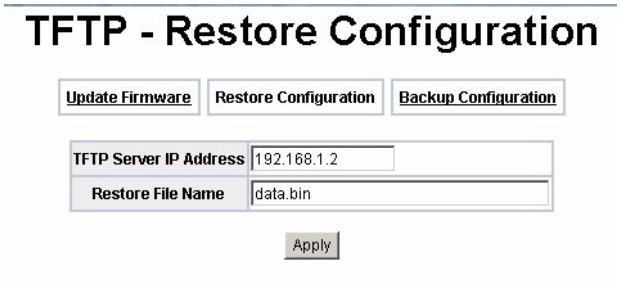


Abbildung 5-8: Oberfläche zur Wiederherstellung der Konfiguration

5.9 Backup-Konfiguration

Speichern Sie den aktuellen EEPROM-Wert des Switch auf dem TFTP-Server. Gehen Sie dann auf die Seite zur Wiederherstellung über TFTP, um den EEPROM-Wert wiederherzustellen.

- ***TFTP SERVER IP ADDRESS:*** Geben Sie die IP-Adresse des TFTP-Servers ein.
- ***BACKUP FILE NAME:*** Geben Sie den Namen der Konfigurationsdatei ein.
- Klicken Sie auf **Apply**.

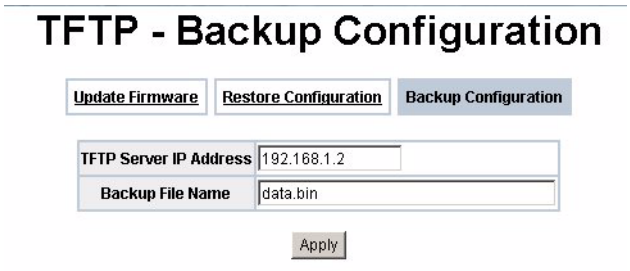


Abbildung 5-9: Oberfläche zur Backup-Konfiguration

5.10 Konfiguration des System Log

Unter diesem Menüpunkt können Sie den Systemereignismodus konfigurieren, den Sie protokollieren wollen, sowie die System Log IP-Adresse.

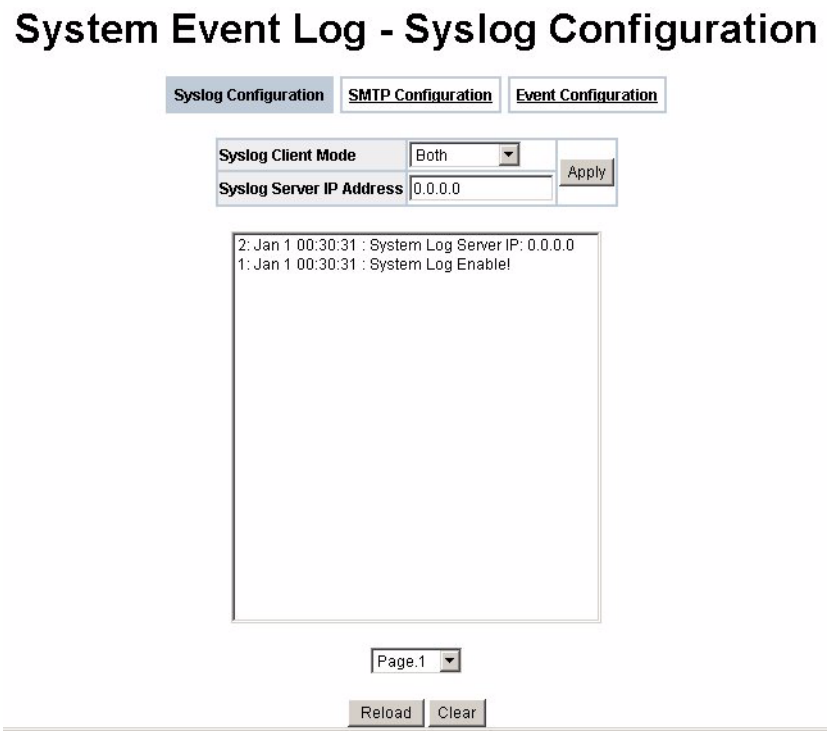


Abbildung 5-10: Oberfläche zur Konfiguration des System Log

- ***System Log Client Mode:*** Wählen Sie den System Log Modus aus – nur Client, nur Server oder beides.
- ***System Log Server IP Address:*** Weisen Sie dem System Log Server die IP-Adresse zu.
- Klicken Sie auf **Reload**, um die Ereignisprotokolle neu zu laden.

- Klicken Sie auf **Clear**, um alle aktuellen Ereignisprotokolle zu löschen.

5.11 SMTP-Konfiguration

Legen Sie die IP-Adresse des Mail Servers, den Mail Account, das Passwort für den Account und einen E-Mail Account zur Weiterleitung fest, unter denen Sie Warnhinweise bei definierten Ereignissen erhalten.

- ***EMAIL ALERT:*** Aktiviert bzw. deaktiviert Warnhinweise per E-Mail.
- ***SMTP SERVER IP ADDRESS:*** Legt die IP-Adresse des Mail Servers fest (diese Funktion ist verfügbar, wenn Warnhinweise per E-Mail aktiviert worden sind).
- ***AUTHENTICATION:*** Klicken Sie das Ankreuzfeld an, um den E-Mail Account und das Passwort zur Authentifizierung zu aktivieren und zu konfigurieren (diese Funktion ist verfügbar, wenn Warnhinweise per E-Mail aktiviert worden sind).
- ***MAIL ACCOUNT:*** Definieren Sie den E-Mail Account, auf dem Sie Warnhinweise empfangen möchten, z.B. johnadmin@123.com. Der E-Mail Account muss auf dem Mail Server existieren, den Sie in der Spalte für IP-Adressen der SMTP-Server festgelegt haben.
- ***PASSWORD:*** Das Passwort des E-Mail Accounts
- ***CONFIRM PASSWORD:*** Bestätigung des Passworts
- ***RCPT E-MAIL ADDRESS 1 - 6:*** Sie können bis zu 6 Mail Accounts definieren, auf denen Sie Warnhinweise empfangen können.
- Klicken Sie auf **Apply**.

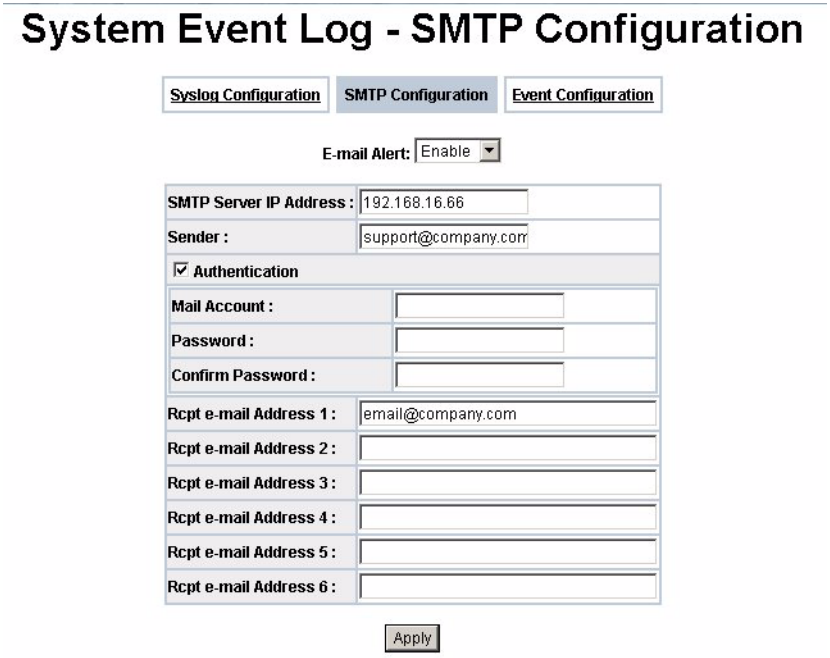


Abbildung 5-11: Oberfläche zur SMTP-Konfiguration

5.12 Konfiguration von Ereignissen

Wählen Sie die System Log- und SMTP-Ereignisse aus. Wenn ausgewählte Ereignisse auftreten, legt das System Protokollinfomationen ab. Sie können auch Protokoll- und SMTP-Ereignisse pro Port auswählen.

- ***SYSTEM EVENT SELECTION:*** Sie haben 4 Auswahlmöglichkeiten – Kaltstart des Geräts, Status der Netzspannung, fehlgeschlagene SNMP-Authentifizierung und Änderung der X-Ring-Topologie. Wählen Sie das entsprechende Ankreuzfeld aus. Wenn ausgewählte Ereignisse auftreten, legt das System Protokollinfomationen ab.

- Device cold start: Wenn das Gerät einen Kaltstart durchführt, dann legt das System ein Log Event (protokolliertes Ereignis) an.
- Device warm start: Wenn das Gerät einen Warmstart durchführt, dann legt das System ein Log Event an.
- Authentication Failure: Wenn eine Authentifizierung über SNMP fehlschlägt, dann legt das System ein Log Event an.
- X - Ring topology change: Wenn sich die X-Ring-Topologie ändert, dann legt das System ein Log Event an.

- Klicken Sie auf **Apply**.

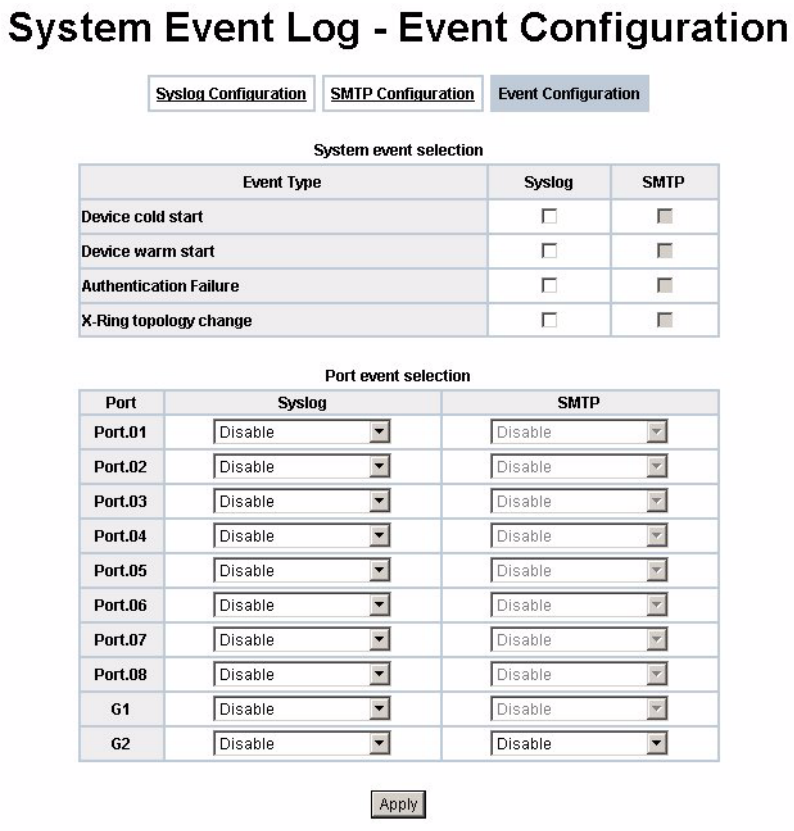


Abbildung 5-12: Oberfläche zur Konfiguration von Ereignissen

- ***PORT EVENT SELECTION:*** Wählen Sie die Ereignisse pro Port und die SMTP-Ereignisse pro Port aus. Sie haben 3 Auswahlmöglichkeiten – Verbindung ist aktiv, Verbindung ist nicht aktiv oder beides. Wenn Sie die Option deaktivieren, bedeutet das, dass kein Ereignis ausgewählt wurde.
  - ***LINK UP:*** Das System erstellt eine Protokollnachricht, wenn die Verbindung auf dem Port aktiv ist.
  - ***LINK DOWN:*** Das System erstellt eine Protokollnachricht, wenn die Verbindung auf dem Port nicht aktiv ist.
  - ***LINK UP & LINK DOWN:*** Das System erstellt eine Protokollnachricht, wenn die Verbindung auf dem Port aktiv oder nicht aktiv ist.

5.13 SNTP-Konfiguration

Dieser Menüpunkt dient zur Konfiguration der SNTP- (Simple Network Time Protocol) Einstellungen.

- ***SNTP CLIENT:*** Aktiviert oder deaktiviert die SNTP-Funktion, mit der ein Zeitabgleich vom SNTP-Server abgefragt wird.
- ***DAYLIGHT SAVING TIME:*** Aktiviert bzw. deaktiviert Abspeichern tagsüber. Wenn das Speichern tagsüber aktiviert wurde, muss der Benutzer dafür ein Zeitfenster tagsüber konfigurieren.
- ***UTC TIMEZONE:*** Legt die lokale Zeitzone fest, in welcher der Switch arbeitet. Die folgende Tabelle gibt eine Übersicht zu den lokalen Zeitzonen.

Lokale Zeitzone	Umrechnung von UTC	Uhrzeit verglichen mit 12:00 Uhr UTC
Zeitzone November	- 1 Stunde	11:00 Uhr
Zeitzone Oscar	- 2 Stunden	10:00 Uhr
ADT - Atlantic Daylight	- 3 Stunden	09:00 Uhr
AST - Atlantic Standard EDT - Eastern Daylight	- 4 Stunden	08:00 Uhr
EST - Eastern Standard CDT - Central Daylight	- 5 Stunden	07:00 Uhr

Lokale Zeitzone	Umrechnung von UTC	Uhrzeit verglichen mit 12:00 Uhr UTC
CST - Central Standard MDT - Mountain Daylight	- 6 Stunden	06:00 Uhr
MST - Mountain Standard PDT - Pacific Daylight	- 7 Stunden	05:00 Uhr
PST - Pacific Standard ADT - Alaskan Daylight	- 8 Stunden	04:00 Uhr
ALA - Alaskan Standard	- 9 Stunden	03:00 Uhr
HAW - Hawaiian Standard	- 10 Stunden	02:00 Uhr
Nome, Alaska	- 11 Stunden	01:00 Uhr
CET - Central European Time FWT - French Winter Time MET - Middle European Time MEWT - Middle European Winter Time SWT - Swedish Winter Time	+ 1 Stunde	13:00 Uhr
EET - Eastern European Time, UdSSR Zone 1	+ 2 Stunden	14:00 Uhr
BT - Bagdad, UdSSR Zone 2	+ 3 Stunden	15:00 Uhr
ZP4 - UdSSR Zone 3	+ 4 Stunden	16:00 Uhr
ZP5 - UdSSR Zone 4	+ 5 Stunden	17:00 Uhr
ZP6 - UdSSR Zone 5	+ 6 Stunden	18:00 Uhr
WAST - West Australian Standard Time	+ 7 Stunden	19:00 Uhr
CCT – China Coast Time, UdSSR Zone 7	+ 8 Stunden	20:00 Uhr
JST - Japan Standard Time, UdSSR Zone 8	+ 9 Stunden	21:00 Uhr
EAST - East Australian Standard Time GST Guam Standard Time, UdSSR Zone 9	+ 10 Stunden	22:00 Uhr
IDLE - International Date Line NZST - New Zealand Standard Time NZT - New Zealand Time	+ 12 Stunden	Mitternacht

- ***SNTP SEVER URL:*** Legt die IP-Adresse des SNTP-Servers fest.
- ***DAYLIGHT SAVING PERIOD START:*** Legt den Beginn des Zeitfensters fest, in dem tagsüber gesichert wird. Dieser Zeitpunkt variiert von Jahr zu Jahr.

- ***DAYLIGHT SAVING PERIOD END:*** Legt das Ende des Zeitfensters fest, in dem tagsüber gesichert wird. Dieser Zeitpunkt ist von Jahr zu Jahr verschieden.
- ***DAYLIGHT SAVING OFFSET (MINS):*** Legt den zeitlichen Versatz fest.
- ***SWITCH TIMER:*** Gibt die aktuelle Zeit auf dem Switch an.
- Klicken Sie auf **Apply**.

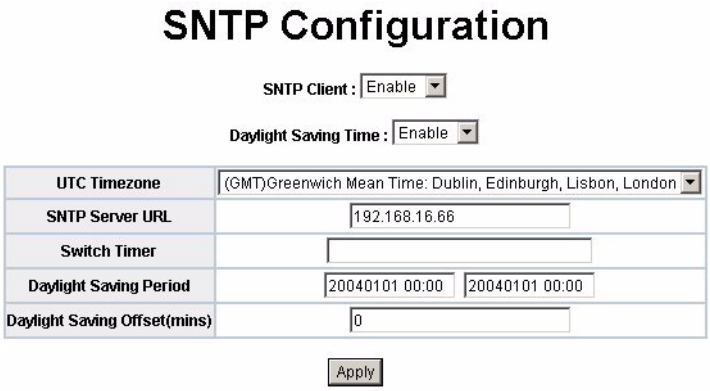


Abbildung 5-13: Oberfläche zur SNTP-Konfiguration

5.14 IP-Sicherheit

Die Funktion IP-Sicherheit ermöglicht es dem Benutzer, bis zu 10 spezifische IP-Adressen zu vergeben, über die über einen Web-Browser auf den Switch zugegriffen werden kann. Damit wird das Switch Management sicherer gemacht.

- ***IP SECURITY MODE:*** Wenn die Option im Modus *Enable* (aktiviert) verwendet wird, dann sind die Ankreuzfelder *Enable HTTP Server* und *Enable Telnet Server* verfügbar, mit denen der HTTP- und Telnet-Server aktiviert werden können.

- ***Enable HTTP Server:*** Wenn Sie dieses Ankreuzfeld angeklickt haben, dann können die IP-Adressen im Sicherheits-IP-Adressbereich von IP1 bis IP10 über HTTP auf den Switch zugreifen.
- ***Enable Telnet Server:*** Wenn Sie dieses Ankreuzfeld angeklickt haben, dann können die IP-Adressen im Sicherheits-IP-Adressbereich von IP1 bis IP10 über Telnet auf den Switch zugreifen.
- ***Security IP 1 - 10:*** Weist bis zu 10 spezifische IP-Adressen zu. Es ist nur über diese 10 IP-Adressen möglich, über den Web-Browser auf den Switch zuzugreifen und ihn zu managen.
- Klicken Sie auf die Schaltfläche **Apply**, um die Konfiguration zu aktivieren.

Hinweis

Denken Sie daran, die Konfiguration mit "Save Configuration" zu sichern. Andernfalls geht die neue Konfiguration verloren, wenn die Stromzufuhr zum Switch unterbrochen oder ausgeschaltet wird.

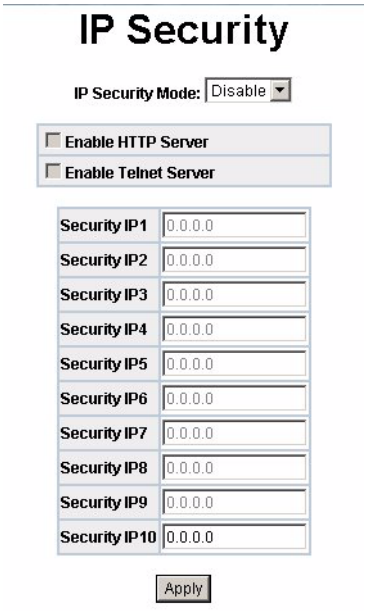


Abbildung 5-14: Oberfläche IP-Sicherheit

5.15 Benutzerauthentifizierung

Unter diesem Menüpunkt können Sie den Benutzernamen und das Passwort für das Web Management Login ändern.

- ***USER NAME:*** Geben Sie den neuen Benutzernamen ein (der standardmäßig gesetzte Name ist "admin").
- ***PASSWORD:*** Geben Sie das neue Passwort ein (das standardmäßig gesetzte Passwort ist "funkwerk").
- ***CONFIRM PASSWORD:*** Geben Sie das neue Passwort noch einmal ein.
- Klicken Sie auf **Apply**.

Abbildung 5-15: Oberfläche Security Manager

5.16 Portstatistik

Die folgenden Informationen bilden die aktuellen Portstatistikinformationen.

- Klicken Sie auf die Schaltfläche **Clear**, um alle Zähler zu löschen.

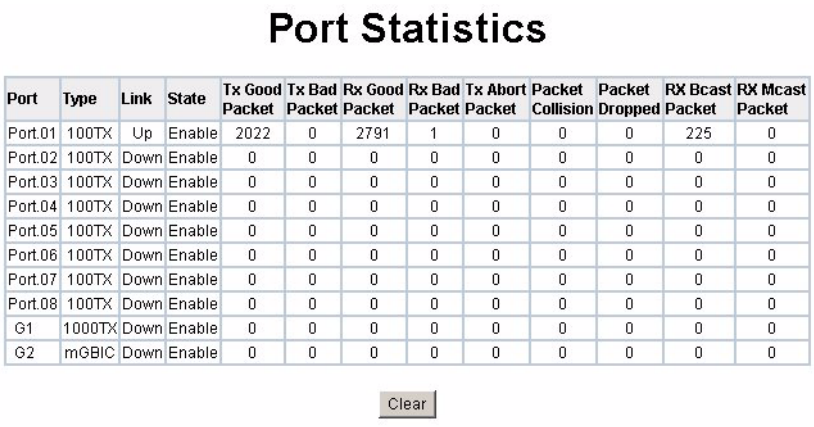
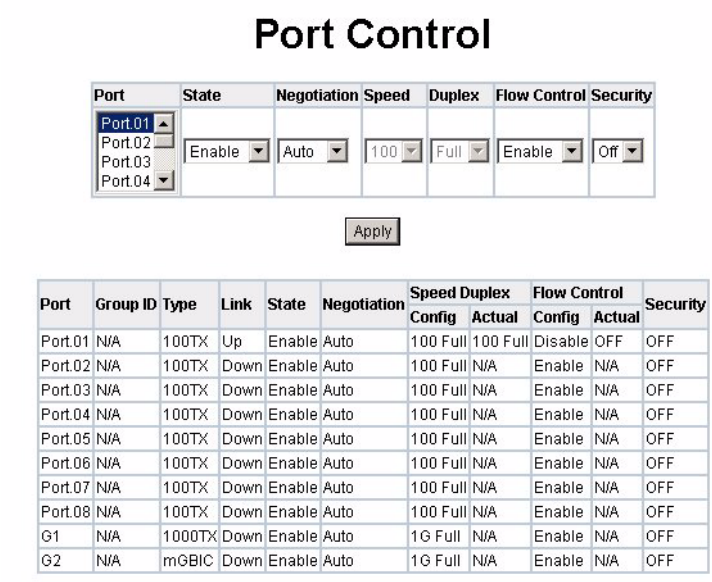

Port Statistics
Port Type Link State Tx Good Packet Tx Bad Packet Rx Good Packet Rx Bad Packet Tx Abort Packet Packet Collision Packet Dropped RX Bcast Packet RX Mcast Packet
Port.01 100TX Up Enable 2022 0 2791 1 0 0 0 225 0
Port.02 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.03 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.04 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.05 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.06 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.07 100TX Down Enable 0 0 0 0 0 0 0 0 0
Port.08 100TX Down Enable 0 0 0 0 0 0 0 0 0
G1 1000TX Down Enable 0 0 0 0 0 0 0 0 0
G2 mGBIC Down Enable 0 0 0 0 0 0 0 0 0
Clear

Abbildung 5-16: Portstatistik

5.17 Konfiguration der Portsteuerung

Prüfen Sie den Status jedes Ports, der über Benutzereinstellungen festgelegt wird, sowie die entsprechenden Ergebnisse.

- ***PORT***: Wählen Sie den Port aus, den Sie konfigurieren möchten.
- ***STATE***: Aktueller Portstatus: Der Port kann auf den Modus aktiviert oder deaktiviert gesetzt werden. Wenn der Port deaktiviert ist, werden hier keine Pakete empfangen oder versendet.
- ***NEGOTIATION***: Hiermit legen Sie den Status der Autonegotiation auf diesem Port fest.
- ***SPEED***: Hier legen Sie die Geschwindigkeit des Port Links fest.
- ***DUPLEX***: Hier legen Sie den Vollduplex- oder Halbduplex-Modus für den Port fest.
- ***FLOW CONTROL:*** Hier können Sie die Flow Control im Vollduplex-Modus als *Symmetric* (symmetrisch) oder *Asymmetric* (asymmetrisch) festsetzen. Die Standardeinstellung ist *Disable* (deaktiviert).
- ***SECURITY***: Wenn diese Option aktiviert ist, dann akzeptiert der Port nur eine MAC-Adresse.
- Klicken Sie auf **Apply**.



Port	Group ID	Type	Link	State	Negotiation	Speed Duplex		Flow Control		Security
						Config	Actual	Config	Actual	
Port.01	N/A	100TX	Up	Enable	Auto	100 Full	100 Full	Disable	OFF	OFF
Port.02	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.03	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.04	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.05	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.06	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.07	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
Port.08	N/A	100TX	Down	Enable	Auto	100 Full	N/A	Enable	N/A	OFF
G1	N/A	1000TX	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF
G2	N/A	mGBIC	Down	Enable	Auto	1G Full	N/A	Enable	N/A	OFF

Abbildung 5-17: Oberfläche Portsteuerung

5.18 Port Trunk

Das Link Aggregation Control Protocol (LACP) ermöglicht den standardisierten Informationsaustausch zwischen Partnersystemen auf einer Verbindung. Damit wird es den Link Aggregation Control Instances der beiden Systeme ermöglicht, die Identität der Link Aggregation Group auszuhandeln, zu welcher der Link gehört, den Link dieser Link Aggregation Group zuzuordnen und sicherzustellen, dass der Empfang und die Übertragung von Daten auf diesem Link ordnungsgemäß ablaufen. Durch Trunk-Gruppen können 8 hintereinander angeordnete Ports zu einer einzigen dezidierten Verbindung zusammengefasst werden. Mit diesem Leistungsmerkmal kann die Bandbreite erweitert werden, die einem Gerät im Netzwerk zur Verfügung gestellt wird. LACP erfordert den Vollduplex-Modus. Weitere Details finden Sie im Standard IEEE 802.3ad.

5.18.1 Einstellungen zur Trunk-Gruppe

- ***System Priority:*** Dieser Wert wird verwendet, um ein aktives LACP zu kennzeichnen. Der Switch mit dem niedrigsten Wert hat die höchste Priorität und wird als aktives LACP ausgewählt.
- ***Group ID:*** Es gibt 3 Trunk-Gruppen, die konfiguriert werden können. Wählen Sie die "Group ID" aus und klicken Sie auf **Select**.
- ***LACP:*** Wenn diese Option aktiviert ist, dann ist die Gruppe eine statische LACP-Trunk-Gruppe. Wenn diese Option nicht aktiviert ist, dann ist die Gruppe eine statische, lokale Trunk-Gruppe. Alle Ports unterstützen dynamische LACP Trunk-Gruppen. Wenn eine Verbindung zu einem Gerät aufgebaut wird, das LACP unterstützt, dann wird automatisch eine dynamische LACP-Trunk-Gruppe gebildet.
- ***Work ports:*** Maximal 4 Ports können gleichzeitig gebündelt werden. Wird eine statische LACP-Trunk-Gruppe konfiguriert, dann befinden sich die überzähligen Ports im Standby-Modus und werden der Gruppe hinzugefügt, wenn ein Work Port ausfällt. Bei lokalen, statischen Trunk-Gruppen muss die Anzahl der Ports der Anzahl der Member Ports der Gruppe entsprechen.
- Wählen Sie die Ports aus, die in die Trunk-Gruppe aufgenommen werden sollen. Maximal 4 Ports können gleichzeitig gebündelt werden.
- Klicken Sie auf die Schaltfläche **Add**, um einen Port hinzuzufügen.
- Um Ports zu entfernen, klicken Sie auf die Schaltfläche **Remove**.
- Durch Klicken auf die Schaltfläche **Apply** erzeugen Sie eine Trunk-Gruppe.
- Um eine Trunk-Gruppe zu löschen, wählen Sie die ID der Gruppe aus und klicken Sie auf die Schaltfläche **Delete**.

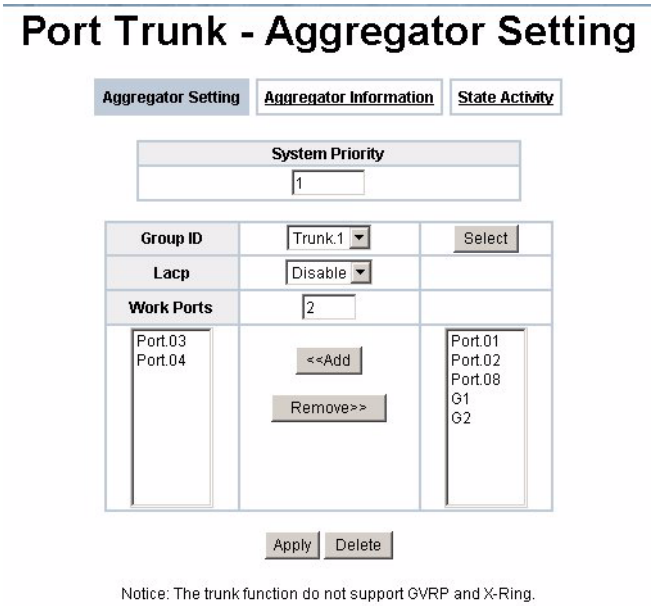


Abbildung 5-18: Oberfläche mit Einstellungen zur Leitungsbündelung am Port

5.18.2 Informationen zur Leitungsbündelung

Wenn LACP-Leitungsbündelung eingestellt ist, dann werden die entsprechenden Informationen hier angezeigt.

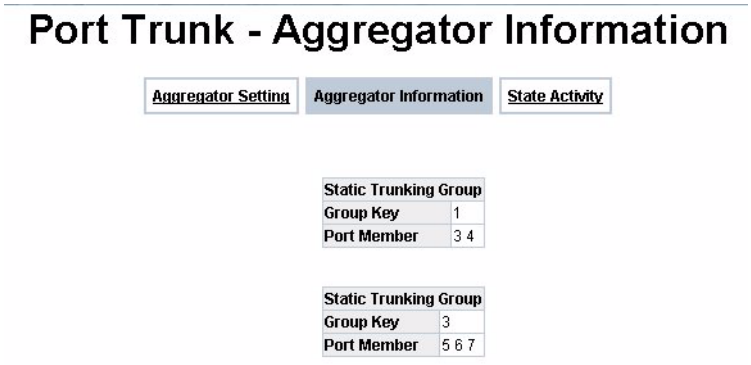


Abbildung 5-19: Oberfläche mit Informationen zur Leitungsbündelung am Port

5.18.3 Aktivitätsstatus

Nachdem Sie LACP-Leitungsbündelung eingestellt haben, konfigurieren Sie den Aktivitätszustand des Ports.

- ***ACTIVE***: Der Port versendet automatisch LACP-Protokoll-Pakete.
- ***PASSIVE***: Der Port versendet nicht automatisch LACP-Protokoll-Pakete. Er antwortet nur, wenn er ein LACP-Protokoll-Paket von einem Gerät auf der Gegenseite empfängt.
- Klicken Sie auf die Schaltfläche **Apply**, um die Einstellung zu aktivieren.

Hinweis

1. Ein Link, der über entweder zwei aktive LACP-Ports oder einen aktiven Port verfügt, kann dynamische LACP-Leitungsbündelung durchführen.
2. Verfügt ein Link über zwei passive LACP-Ports, kann er keine dynamische LACP-Leitungsbündelung durchführen, da beide Ports auf ein LACP-Protokoll-Paket warten, dass von einem Gerät auf der Gegenseite gesendet wird.
3. Wurde auf der Gegenstelle des Trunks LACP aktiviert, dann wird der Status automatisch auf "aktiv" gesetzt, sobald der Benutzer einen Trunk Port auswählt.

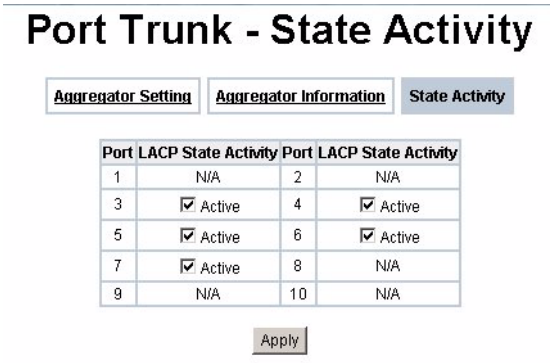


Abbildung 5-20: Leitungsbündelung – Oberfläche Aktivitätsstatus

5.19 Port Mirroring

Port Mirroring (Portspiegelung) ist eine Methode zur Überwachung von Datenverkehr in geswitchten Netzwerken. Datenverkehr, der über verschiedene Ports läuft, kann von einem bestimmten Port aus überwacht werden. Das bedeutet, dass Datenverkehr, der auf dem überwachten Port empfangen oder versendet wird, auf dem gespiegelten Port dupliziert wird.

- ***Destination Port:*** Alle überwachten Ports können von dem gespiegelten Port aus eingesehen werden. Sie können den gespiegelten Port an einen LAN-Analyzer oder an Netxray anschliessen.
- ***Source Port:*** Der Port, den der Benutzer überwachen will. Der Datenverkehr auf allen überwachten Ports wird auf den gespiegelten Port (Zielport) kopiert. Der Benutzer kann maximal 9 Ports zur Überwachung am Switch auswählen. Der Benutzer kann den Port, den er überwachen möchte, im Mirror-Modus auswählen. Sie können folgende Mirror-Zustände auswählen: RX (Empfangen), TX (Übertragen) oder beides.
- Klicken Sie auf **Apply**.
- Um die Einstellung zurückzusetzen, klicken Sie auf die Schaltfläche **Clear**, bevor Sie die Einstellungen aktivieren.

Hinweis

Um die Funktion zu deaktivieren, wählen Sie als Quellport keinen Port aus.

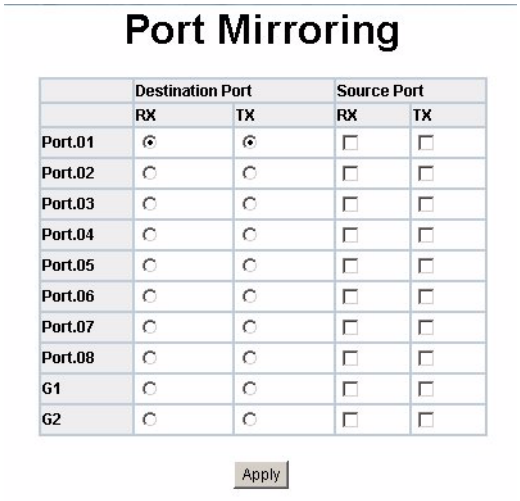


Abbildung 5-21: Oberfläche Port Mirroring

5.20 Begrenzung der Bandbreite

Legen Sie für jeden Port die Bandbreite fest, mit der Daten übertragen werden, sowie die Begrenzung der übertragenen Pakete nach Paketart.

- ***INGRESS LIMIT PACKET TYPE:*** Wählen Sie die Paketart aus, die Sie filtern wollen. Sie können zwischen allen Paketarten, Broadcast-/Flooded Unicast-Paketen, Broadcast/Multicast-Paketen und nur Broadcast-Paketen wählen. Die Varianten Broadcast-/Multicast-/Flooded Unicats-Pakete, Broadcast-/Multicast-Pakete und Broadcast-Pakete werden nur für eingehende Pakete unterstützt. Die ausgehende Datenrate unterstützt alle Paketarten.

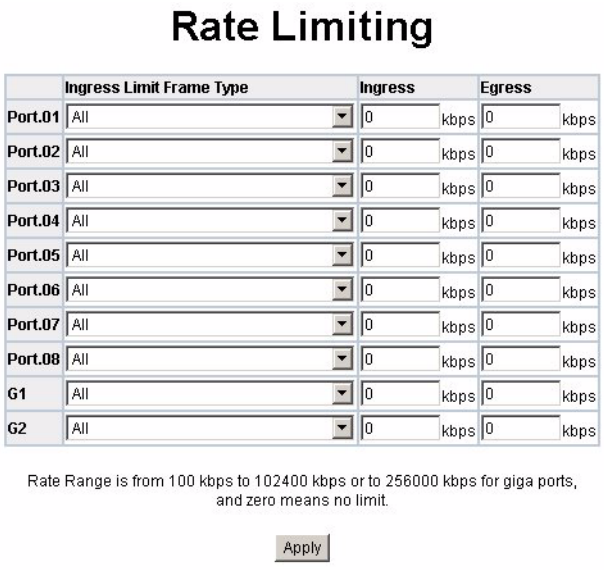


Abbildung 5-22: Oberfläche zur Begrenzung der Bandbreite

- Alle Ports unterstützen die Steuerung der eingehenden und ausgehenden Datenrate an den Ports. Wenn man z.B. für Port 1 eine Datenrate von 10 Mbit/s annimmt, dann kann der Benutzer die effektive ausgehende Datenrate dieses Ports auf 1 Mbit/s festlegen und die eingehende Datenrate auf 500 Kbit/s. Der Switch steuert die eingehende Datenrate über den Paketzähler und hält so die vorgegebene Datenrate ein.
  - ***INGRESS:*** Tragen Sie die effektive eingehende Datenrate für den Port ein (Der Standardwert ist "0".).
  - ***EGRESS:*** Tragen Sie die effektive ausgehende Datenrate für den Port ein (Der Standardwert ist "0".).
- Klicken Sie auf die Schaltfläche **Apply**, um die Einstellung zu aktivieren.

5.21 VLAN-Konfiguration

Ein Virtual LAN (VLAN) ist eine logische Netzwerkgruppe, welche die Broadcast Domain begrenzt. Sie ermöglicht es, den Verkehr im Netzwerk zu isolieren, so dass nur VLAN-Teilnehmer Datenverkehr von Teilnehmern desselben VLAN empfangen. Der Aufbau eines VLAN von einem Switch aus entspricht vom Prinzip her der Anbindung einer Gruppe von Netzwerkgeräten an einen anderen Layer 2 Switch. Alle Netzwerkgeräte sind jedoch nach wie vor physikalisch an demselben Switch angeschlossen.

Der Switch unterstützt Port-basiertes, 802.1Q (Tag-basiert) und Protokoll-basiertes VLAN über die Web Management Webseite. Bei der Standardkonfiguration ist die VLAN-Funktion deaktiviert ("disable").

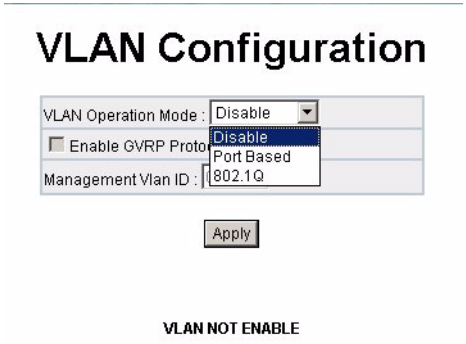


Abbildung 5-23: Oberfläche zur VLAN-Konfiguration

5.21.1 Port-basiertes VLAN

Pakete werden nur zwischen Teilnehmern derselben VLAN-Gruppe versendet. Beachten Sie, dass alle Ports, die nicht ausgewählt wurden, so behandelt werden, als gehörten sie zu einem anderen, nicht verbundenen VLAN. Ist die Funktion Port-basiertes VLAN aktiviert, dann wird das VLAN-Tagging ignoriert.

Damit ein Endgerät Pakete in andere VLANs versenden kann, muss es entweder in der Lage sein, die zu versendenden Pakete mit VLAN Tags zu versehen, oder es muss an eine VLAN-fähige Bridge angeschlossen sein. Diese Bridge muss Pakete mit anderen VLAN-IDs klassifizieren und taggen können. Das gilt nicht nur für VLAN-IDs, die auf standardisierten PVIDs basieren, sondern auch für alle anderen Informationen, die sich auf das Paket beziehen, also z.B. das Protokoll.

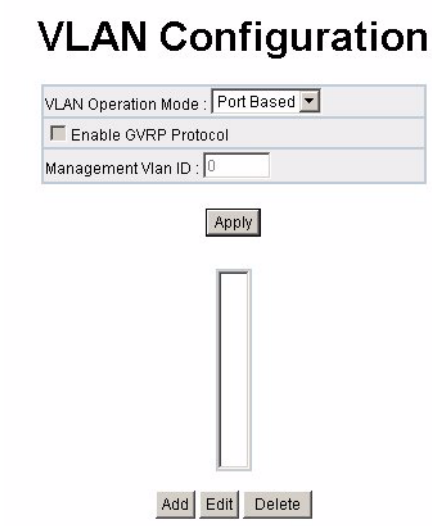


Abbildung 5-24: Oberfläche zu Port-basierten VLANs

- Durch das Klicken auf die Schaltfläche **Apply** erzeugen Sie eine eine neue VLAN-Gruppe.

- Geben Sie den Namen der Gruppe und die VLAN-ID ein und wählen Sie die Teilnehmer der VLAN-Gruppe aus.
- Klicken Sie auf **Apply**.

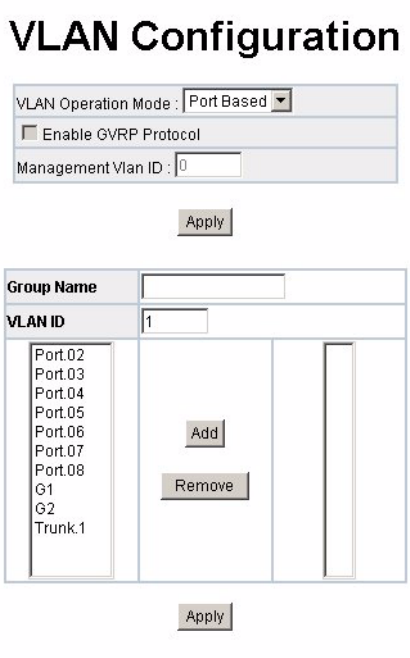


Abbildung 5-25: Oberfläche zum Hinzufügen eines Port-basierten VLANs

- Die VLAN-Gruppe wird angezeigt.
- Um ein VLAN zu löschen, klicken Sie auf die Schaltfläche **Delete**.
- Sie können auch auf die Schaltfläche **Edit** klicken,

5.21.2 802.1Q VLAN

Der Standard IEEE 802.1Q spezifiziert Tag-basierte VLANs. Auf der Basis dieser Standardisierung ist es möglich, ein VLAN aufzubauen, das Switches verschiedener Hersteller umfasst. VLANs, die gemäß dem Standard IEEE 802.1Q konfiguriert werden, fügen Tags in Ethernet Frames ein. Der Tag enthält einen VLAN-Identifier (VID), der die VLAN-Nummer angibt.

Der Benutzer kann Tag-basierte VLANs aufbauen und dabei das GVRP-Protokoll aktivieren oder deaktivieren. Es gibt 256 VLAN-Gruppen, die konfiguriert werden können. Wenn Sie das 802.1Q VLAN aktivieren, dann gehören alle Ports des Switch zu dem Standard-VLAN. Die VID ist 1. Das Standard-VLAN kann nicht gelöscht werden.

GVRP ermöglicht die automatische Konfiguration eines VLANs zwischen Switch und Netzknoten. Wenn der Switch an ein Gerät angeschlossen ist, auf dem GVRP aktiviert ist, dann können Sie eine GVRP-Anfrage versenden und dabei die VID des VLAN verwenden, die auf dem Switch definiert wurde. Der Switch wird das Gerät dann automatisch in das bestehende VLAN aufnehmen.

802.1Q-Konfiguration

- ***Enable GVRP Protocol:*** Überprüfen Sie das Ankreuzfeld, um das GVRP-Protokoll zu aktivieren.
- Wählen Sie den Port aus, den Sie konfigurieren möchten.
- ***Link Type:*** Es gibt 3 Arten von Links: der Access Link, Trunk Link und der Hybrid Link.
- ***Untagged VID:*** Weisen Sie die VID dem nicht-getaggten Frame zu.
- ***Tagged VID:*** Weisen Sie die VID dem getaggten Frame zu.
- Klicken Sie auf **Apply**.
- Alle Porteinstellungen werden in der untenstehenden Tabelle dargestellt.

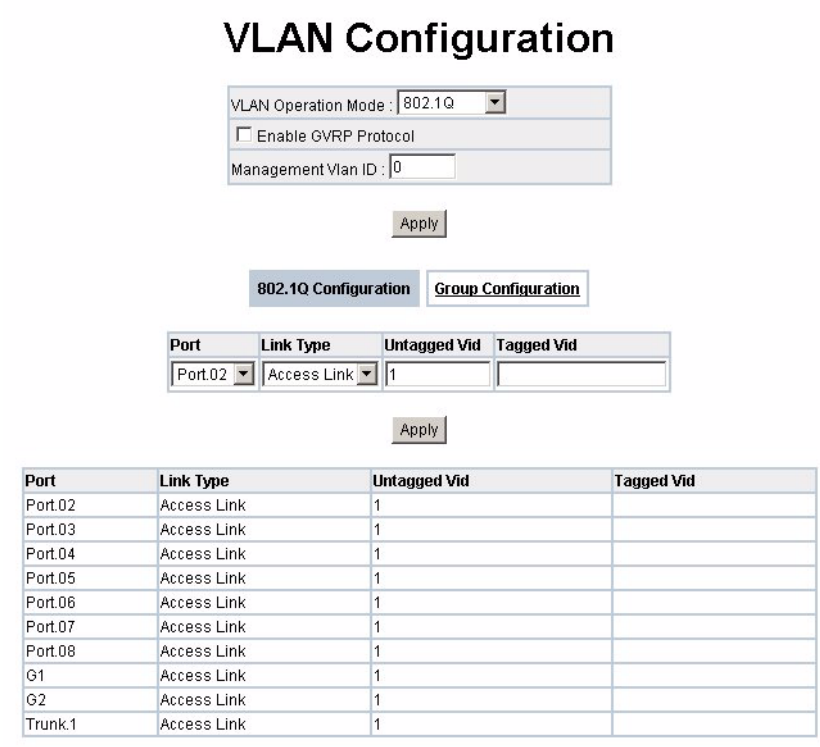


Abbildung 5-26: Oberfläche zur 802.1Q-VLAN-Konfiguration

Konfiguration von Gruppen

Bearbeiten der VLAN-Gruppe

- Wählen Sie die VLAN-Gruppe in der Tabelle aus.
- Klicken Sie auf **Apply**.

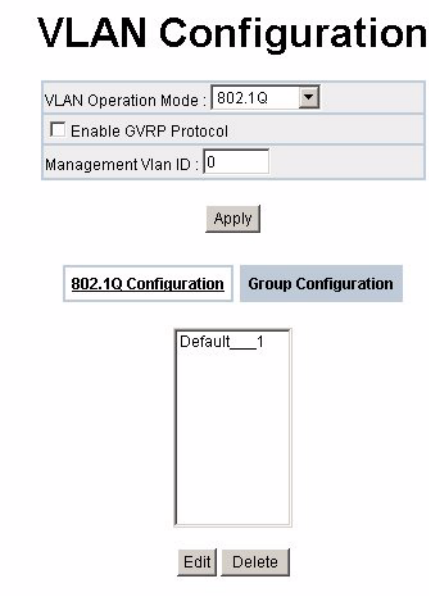


Abbildung 5-27: Oberfläche zur Konfiguration von Gruppen

- Der Benutzer kann die VLAN-Gruppe und die VLAN ID modifizieren.
- Klicken Sie auf **Apply**.

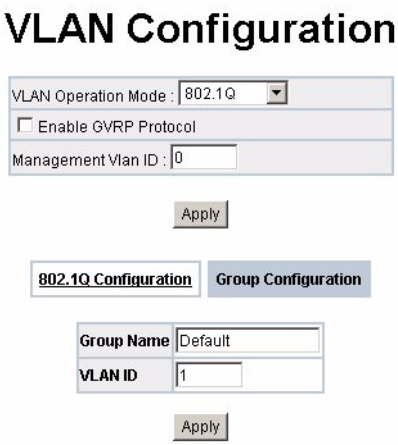


Abbildung 5-28: Oberfläche zur Konfiguration von Gruppen

5.22 Rapid Spanning Tree

Das Rapid Spanning Tree Protocol (RSTP) ist eine Weiterentwicklung des Spanning Tree Protocols. Es bietet eine schnellere Spanning-Tree-Konvergenz nach einer Änderung der Topologie. Das System unterstützt auch STP und ist in der Lage, selbstständig angebundene Geräte zu erkennen, die das STP- oder RSTP-Protokoll benutzen.

5.22.1 RSTP-Systemkonfiguration

- Die Root Bridge Information des Spanning Tree Protokolls wird hier angezeigt.
- RSTP-Status ändern:
  - ***RSTP MODE:*** Hier aktivieren oder deaktivieren Sie die RSTP-Funktion, bevor Sie weiterführende Parameter konfigurieren.
  - ***PRIORITY (0-61440):*** Dieser Wert wird verwendet, um die Root Bridge zu kennzeichnen. Die Bridge mit dem niedrigsten Wert hat die höchste Priorität und wird als Root Bridge ausgewählt. Wenn sich die Werte ändern, muss der Benutzer den Switch neu starten, um die Pfadprioritäts-Nummer zuzuweisen. Gemäß dem Standardprotokoll muss der Wert ein Vielfaches von 4096 sein.
  - ***HELLO TIME (1-10):*** Festlegung eines Zeitfensters von 1 bis 10 s, in dem der Switch Hello Broadcasts an andere Switches versendet.
  - ***MAX AGE (6-40):*** Dauer in Sekunden (6 bis 40), während der Protokollinformationen, die auf einem Port empfangen werden, vom Switch abgespeichert werden.
  - ***FORWARD DELAY TIME (4-30):*** Dauer in Sekunden (4 bis 30), die jeder Listening- (Zuhören) und Learning- (Lernen)Zustand dauert, bevor der Port mit der Weiterleitung beginnt.
- Klicken Sie auf **Apply**.

Hinweis

Befolgen Sie die untenstehende Regel bei der Konfiguration der Maximum Age (maximale Lebensdauer), der Hello Time und der Forward Delay Time (zeitlicher Versatz vor Weiterleitung).

2 x (WERT FORWARD DELAY TIME -1) > = WERT MAX AGE> =
2 x (WERT HELLO TIME +1)

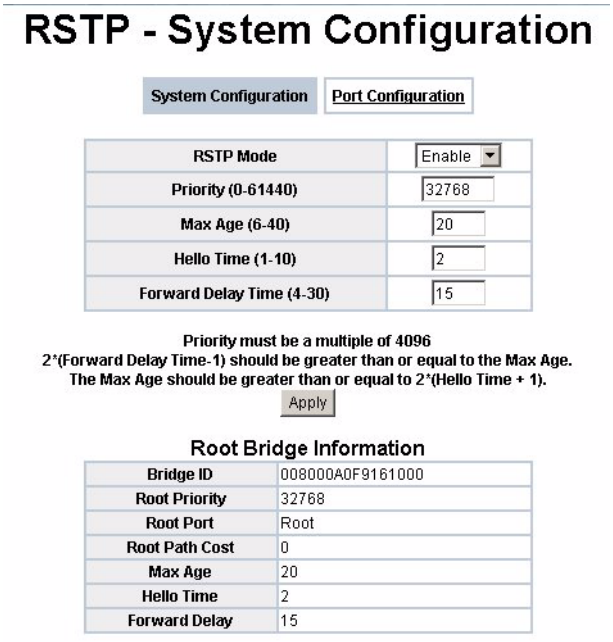


Abbildung 5-29: Oberfläche zur RSTP-Systemkonfiguration

5.22.2 RSTP-Konfiguration pro Port

Konfigurieren Sie die Pfadkosten und die Priorität auf jedem Port.

- Wählen Sie den Port in der entsprechenden Spalte aus.
- ***PATH COST:*** Pfadkosten von der übertragenden Brücke am angegebenen Port zur anderen Brücke. Geben Sie eine Zahl zwischen 1 und 200000000 ein.
- ***PRIORITY:*** Legen Sie fest, welcher Port nach Priorität im LAN geblockt werden soll. Geben Sie eine Zahl von 0 bis 240 ein. Der Prioritätswert muss ein Vielfaches von 16 sein.

- ***P2P:*** Die Durchführung einiger Aktionen im Rapid State gemäß RSTP hängt davon ab, ob der entsprechende Port nur mit exakt einer anderen Brücke verbunden werden kann (also über eine Punkt-zu-Punkt LAN-Verbindung angebunden ist) oder ob er mit zwei oder mehr Brücken verbunden werden kann (also über ein Shared Medium LAN-Segment angebunden ist). Mit dieser Funktion können Sie den Status der P2P-Verbindung als Administrator ändern. Der Wert "True" aktiviert P2P. "False" deaktiviert P2P.
- ***EDGE:*** Der Port, der direkt an die Endgeräte angeschlossen ist, kann keinen Bridging Loop im Netzwerk aufbauen. Um den Port als Edge Port (Port im Randbereich des Netzes) zu konfigurieren, setzen Sie den Status des Ports auf den Wert *True*.
- ***STP NEIGHBOR:*** Der Port verwendet mathematische Berechnungen gemäß STP. Der Wert "True" ist nicht in der mathematischen Berechnung enthalten. Der Wert *False* ist in der mathematische Berechnungen gemäß STP enthalten.
- Klicken Sie auf die Schaltfläche **Apply**.

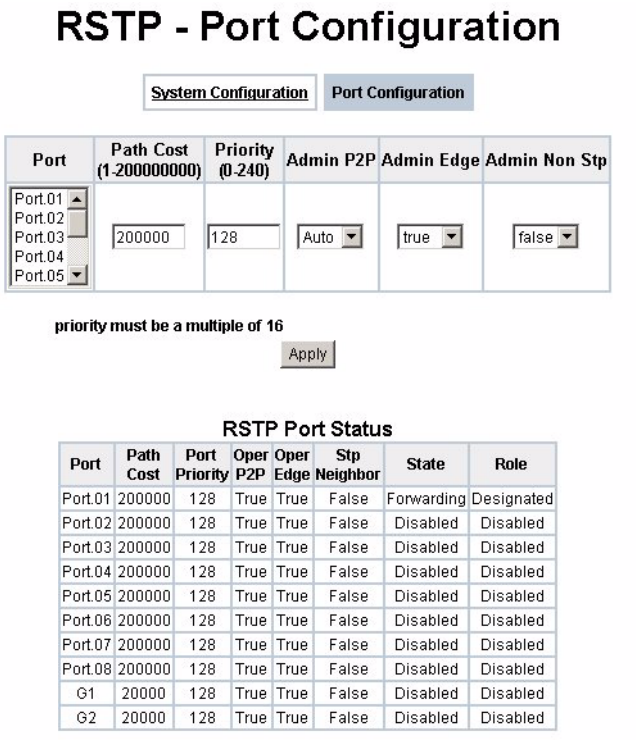


Abbildung 5-30: Oberfläche zur RSTP-Konfiguration pro Port

5.23 SNMP-Konfiguration

Das Simple Network Management Protocol (SNMP) ist ein Protokoll, das dazu dient, Netzknoten (Server, Endgeräte, Router, Switche, Hubs etc.) in einem IP-Netzwerk zu verwalten. SNMP ermöglicht es Netzwerkadministratoren, die Leistung des Netzwerks zu managen, Probleme im Netzwerk zu lokalisieren und zu lösen und eine Erweiterung des Netzwerks zu planen. Netzwerkmanagementsysteme erlangen Kenntnis von Problemen, indem sie Traps oder Informationen über Änderungen von den Netzwerken empfangen, die mit SNMP arbeiten.

5.23.1 Systemkonfiguration

Definiert ein neues Community String Set und entfernt unerwünschte Community Strings.

- ***STRING***: Geben Sie den Namen des Strings ein.
- ***RO***: Read only (nur Lesen). Ermöglicht es Anfragen mit diesem String, Informationen zu MIB-Objekten anzuzeigen.
- ***RW***: Read write (Lese- und Schreibrecht). Ermöglicht es Anfragen mit diesem String, Informationen zu MIB-Objekten anzuzeigen und MIB-Objekte anzulegen.
- Klicken Sie auf die Schaltfläche **Add**.
- Um den von Ihnen definierten Community String wieder zu entfernen, klikken Sie auf die Schaltfläche **Remove**. Der standardmäßig angelegte Community String Set kann nicht entfernt werden.
- Agent Mode: Wählen Sie die SNMP-Version aus, die Sie verwenden möchten.
- Klicken Sie auf die Schaltfläche **Change**, um in den Modus der ausgewählten SNMP-Version zu wechseln.

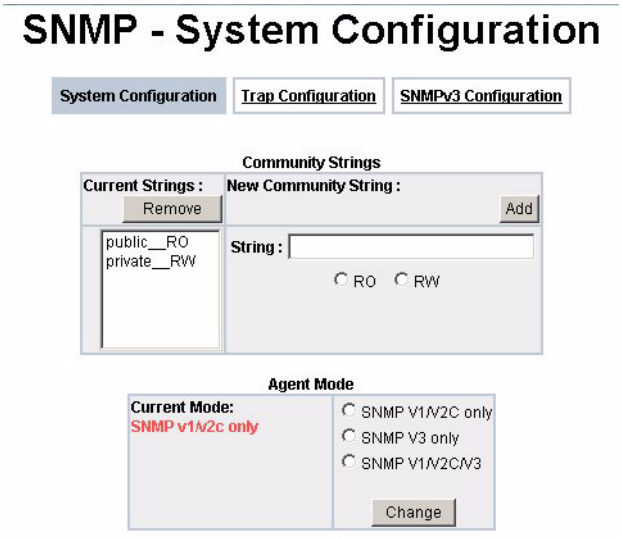


Abbildung 5-31: Oberfläche zur SNMP-Systemkonfiguration

5.23.2 Trap-Konfiguration

Ein Trap Manager ist eine Management Station, die Traps empfängt. Traps sind Systemwarnmeldungen, die der Switch erzeugt. Wenn kein Trap Manager definiert wurde, werden keine Traps erzeugt. Um einen Trap Manager zu erzeugen, geben Sie die IP-Adresse des Endgeräts und einen Community String ein. Definieren Sie die Management Station als Trap Manager, geben Sie die SNMP Community Strings ein und wählen Sie die SNMP-Version aus.

- IP Address: Geben Sie die IP-Adresse des Trap Managers ein.
- Community: Geben Sie den Community String ein.
- Trap Version: Wählen Sie die SNMP Trap Version aus: v1 oder v2.
- Klicken Sie auf **Add**.

- Um den von Ihnen definierten Community String wieder zu entfernen, klikken Sie auf die Schaltfläche **Remove**. (Der standardmäßig angelegte Community String kann nicht entfernt werden.)

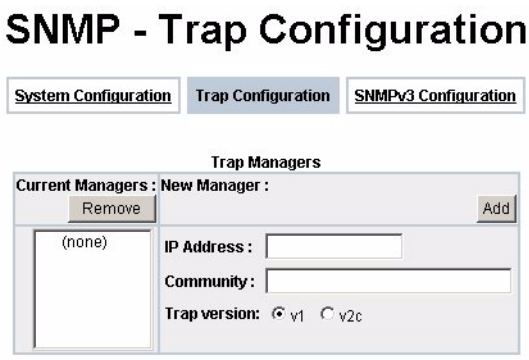


Abbildung 5-32: Oberfläche Trap Manager

5.23.3 SNMPv3-Konfiguration

Konfigurieren der SNMPv3-Funktion

Kontext-Tabelle Weisen Sie der Kontext-Tabelle einen Kontext-Namen zu.

- Klicken Sie auf die Schaltfläche **Add**, um einen Kontext-Namen hinzuzufügen.
- Klicken Sie auf **Remove**, um einen Kontext-Namen zu entfernen.

Benutzerprofil Konfigurieren Sie die SNMPv3-Benutzertabelle.

- ***User ID***: Legen Sie den Benutzernamen fest.
- ***Authentication Password***: Legen Sie das Authentifizierungspasswort fest.
- ***Privacy Password***: Legen Sie das Ihr privates Passwort fest.

- Klicken Sie auf die Schaltfläche **Add**, um einen Kontextnamen hinzuzufügen.
- Klicken Sie auf **Remove**, um einen Kontext-Namen zu entfernen.

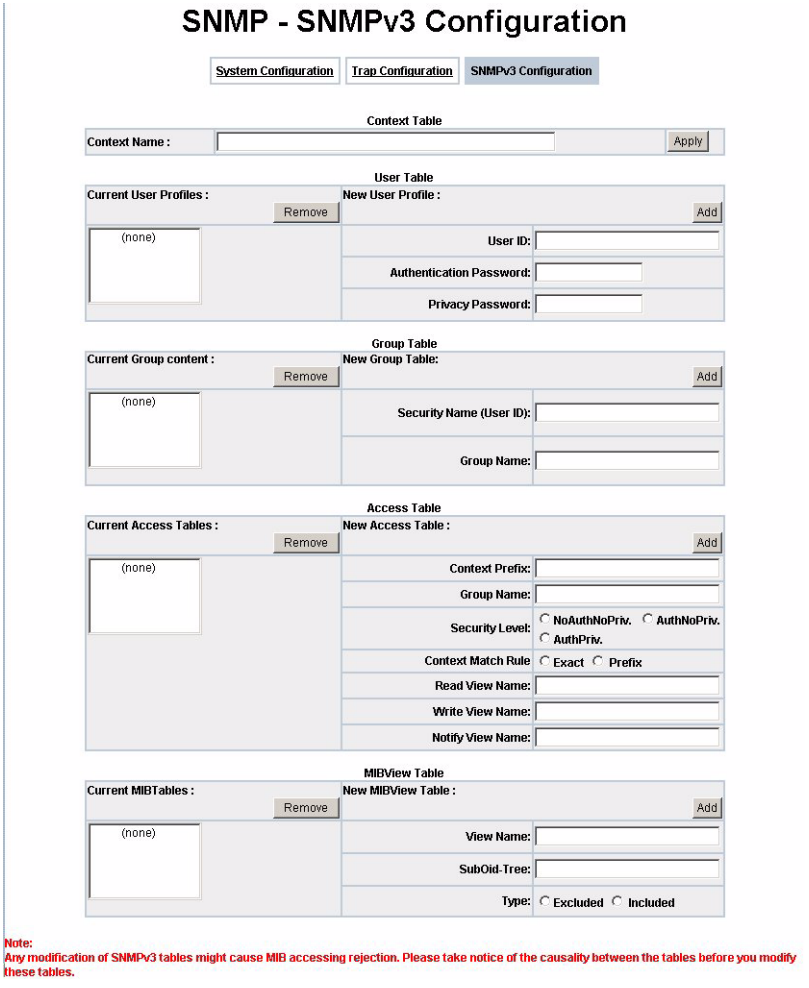


Abbildung 5-33: Oberfläche zur SNMPv3-Konfiguration

Gruppentabelle Konfigurieren Sie die SNMPv3-Gruppentabelle.

- ***Security Name (User ID):*** Weisen Sie den Benutzernamen zu, der in der Benutzertabelle definiert wurde.
- ***Group Name:*** Legen Sie den Namen der Gruppe fest.
- Klicken Sie auf die Schaltfläche **Add**, um einen Kontextnamen hinzuzufügen.
- Klicken Sie auf **Remove**, um einen Kontext-Namen zu entfernen.

Zugangstabelle Konfigurieren Sie die SNMPv3-Zugangstabelle.

- ***Context Prefix:*** Legen Sie den Kontextnamen fest.
- ***Group Name:*** Legen Sie die Gruppe an.
- ***Security Level:*** Wählen Sie den Zugangslevel aus.
- ***Read View Name:*** Definieren Sie die Ansicht "Lesen".
- ***Write View Name:*** Definieren Sie die Ansicht "Schreiben".
- ***Notify View Name:*** Definieren Sie die Ansicht "Benachrichtigen".
- Klicken Sie auf die Schaltfläche **Add**, um einen Kontextnamen hinzuzufügen.
- Klicken Sie auf **Remove**, um einen Kontext-Namen zu entfernen.

MIBview-Tabelle Konfigurieren Sie die MIBview-Tabelle

- ***ViewName:*** Legen Sie den Namen fest.
- ***Sub-Oid Tree:*** Geben Sie die IP-Adresse des Sub-OID-Servers ein.
- ***Type***: Wählen Sie den Typ aus – ausschließen oder mit einschließen.
- Klicken Sie auf die Schaltfläche **Add**, um einen Kontextnamen hinzuzufügen.
- Klicken Sie auf **Remove**, um einen Kontext-Namen zu entfernen.

5.24 QoS-Konfiguration

Konfigurieren Sie die QoS-Policy und die Prioritätseinstellungen, die Prioritätseinstellungen pro Port, die CoS- und die ToS-Einstellungen.

5.24.1 QoS-Policy und Prioritäten

- ***QOS POLICY***: Wählen Sie die QoS-Policy aus.
  - ***USING THE 8,4,2,1 WEIGHT FAIR QUEUE SCHEME:*** Der Switch verwendet eine Gewichtung von 8:4:2:1, um die Prioritäten-Queues von der höchsten zur niedrigsten Queue abzuarbeiten. Beispiel: Das System bearbeitet 80 % des Datenverkehrs einer Queue mit hoher Priorität, 40 % des Verkehrs einer Queue mit mittlerer Priorität, 20 % des Verkehrs einer Queue mit niedriger Priorität und 10 % des Verkehrs der Queue mit der niedrigsten Priorität zu demselben Zeitpunkt. Der Datenverkehr in der Queue mit niedriger Priorität wird nicht übertragen, bis dass der gesamte Datenverkehr der Prioritätsstufen hoch, mittel und normal weitergeleitet worden ist.
  - ***USE THE STRICT PRIORITY SCHEME:*** Es wird immer die Queue mit der höheren Priorität zuerst bedient, es sei denn, diese Queue ist leer.
- ***PRIORITY TYPE:*** An jedem Port können 5 Prioritätsstufen ausgewählt werden. Wenn Sie die Option deaktivieren, bedeutet das, dass keine Prioritätsstufe ausgewählt wird.
  - ***PORT-BASE:*** Die Priorität an dem Port entspricht der standardmäßig zugewiesenen Portpriorität: hoch, mittel, niedrig oder niedrigste Priorität.
  - ***COS ONLY:*** Die Portpriorität entspricht lediglich der zugewiesenen CoS-Priorität.
  - ***TOS ONLY:*** Die Portpriorität entspricht lediglich der zugewiesenen ToS-Priorität.
  - ***COS FIRST:*** Die Portpriorität entspricht zunächst der CoS-Priorität, dann den anderen Prioritätsregeln.
  - ***TOS FIRST:*** Die Portpriorität entspricht zunächst der ToS-Priorität, dann den anderen Prioritätsregeln.
- Klicken Sie auf **Apply**.

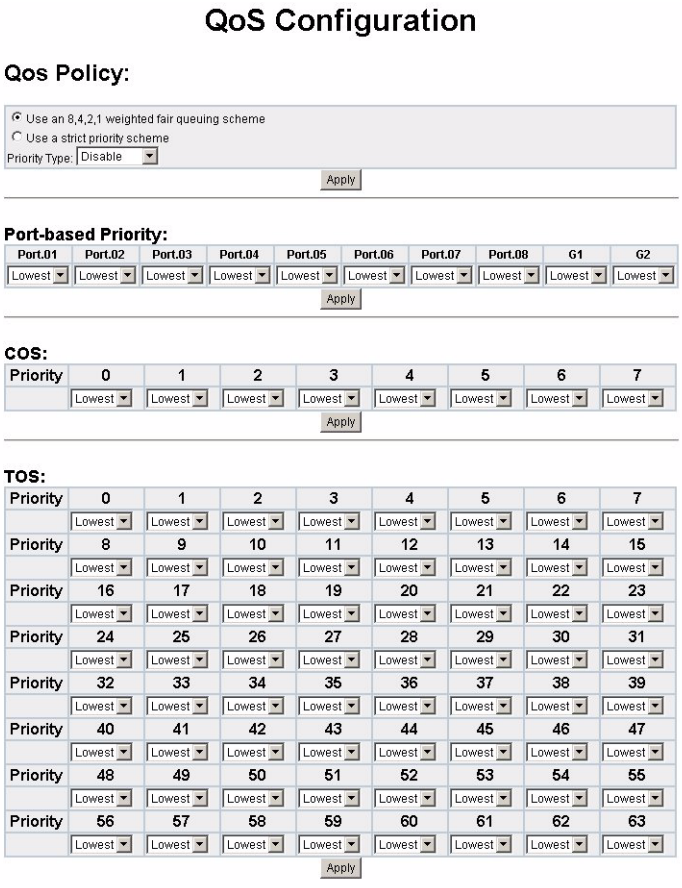

QoS Configuration
Qos Policy:
Use an 8,4,2,1 weighted fair queuing scheme
Use a strict priority scheme
Priority Type: Disable
Apply
Port-based Priority:
Port.01 Port.02 Port.03 Port.04 Port.05 Port.06 Port.07 Port.08 G1 G2
Lowest
Apply
COS:
Priority 0 1 2 3 4 5 6 7
Lowest
Apply
TOS:
Priority 0 1 2 3 4 5 6 7
Priority 8 9 10 11 12 13 14 15
Priority 16 17 18 19 20 21 22 23
Priority 24 25 26 27 28 29 30 31
Priority 32 33 34 35 36 37 38 39
Priority 40 41 42 43 44 45 46 47
Priority 48 49 50 51 52 53 54 55
Priority 56 57 58 59 60 61 62 63
Lowest
Apply

Abbildung 5-34: Oberfläche zur QoS-Konfiguration

5.24.2 Port-basierte Priorität

Konfigurieren Sie die Prioritätsstufe pro Port.

- ***Port 1 - G1& G2:*** Jeder Port verfügt über 4 Prioritätsstufen: hoch, mittel, niedrig und niedrigste Stufe.

- Klicken Sie auf **Apply**.

5.24.3 CoS-Konfiguration

Legen Sie die CoS-Prioritätsstufe fest.

- ***COS PRIORITY:*** Legen Sie die CoS-Prioritätsstufe fest von 0 bis 7 – hoch, mittel, niedrig, niedrigste Stufe.
- Klicken Sie auf **Apply**.

5.24.4 ToS-Konfiguration

Legen Sie die ToS-Prioritätsstufe fest.

- ***TOS PRIORITY***: Das System bietet ToS-Prioritätslevel von 0 bis 63 an. Jeder Level verfügt über 4 Prioritätsstufen: hoch, mittel, niedrig und niedrigste Stufe. Die Standardeinstellung ist "Lowest" (niedrigste Stufe) für jeden Level. Wenn ein IP-Paket empfangen wird, prüft das System den Wert des ToS-Levels, mit dem das Paket empfangen wird. Beispiel: Der Benutzer setzt den ToS-Level auf 25, und damit auf "hoch". Port 1 befolgt ausschließlich die ToS-Prioritäts-Policy. Wenn Port 1 ein Paket empfängt, prüft das System den Wert des ToS-Levels, mit dem das IP-Paket empfangen wird. Wenn der ToS-Wert des empfangenen IP-Pakets 25 ist (Priorität = hoch), dann enstpricht die Priorität des Pakets der höchsten Priorität.
- Klicken Sie auf **Apply**.

5.25 IGMP-Konfiguration

Das Internet Group Management Protocol (IGMP) ist ein internes Protokoll der Internet Protocol (IP) Suite. Das Internet Protocol realisiert Multicast-Datenverkehr durch den Einsatz von Switches, Routern und Hosts, die IGMP unterstützen. Die Verwendung von IGMP ermöglicht es dem Port, IGMP-basierte Anfragen und Nachrichten zu erkennen und IP-Multicast-Verkehr über den

Switch zu verwalten. IGMP verwendet grundsätzlich 3 Arten von Meldungen, wie in der folgenden Tabelle beschrieben:

Meldung	Beschreibung
Query (Anfrage)	Eine Meldung wird von einer anfragenden Einheit (IGMP-Router oder Switch) versendet. Es wird damit eine Antwort von jedem Host angefordert, der zur Multicast-Gruppe gehört.
Report (Bericht)	Dies ist eine Meldung, die ein Host an eine anfragende Einheit verschickt, um damit zu signalisieren, dass der Host Mitglied einer in der Report-Meldung angegebenen Gruppe ist oder dies werden möchte.
Leave Group (Verlasse Gruppe)	Dies ist eine Meldung, die der Host an die anfragende Einheit versendet, um zu signalisieren, dass er nicht mehr Mitglied einer bestimmten Multicast-Gruppe ist.

5.25.1 IGMP-Konfiguration

Wenn der Switch IP Multicast unterstützt, dann kann der Benutzer das IGMP-Protokoll über die erweiterten Einstellungen im Web Management des Switch aktivieren und dann die IGMP-Snooping-Information anzeigen. Der IP-Multicast-Adressbereich erstreckt sich hier von 224.0.0.0 bis 239.255.255.255.

- ***IGMP Protocol:*** Aktiviert bzw. deaktiviert das IGMP-Protokoll.
- ***IGMP Query:*** Aktiviert bzw. deaktiviert IGMP-Abfragefunktion. Die über IGMP abgefragte Information wird unter IGMP-Status angezeigt.
- Klicken Sie auf **Apply**.

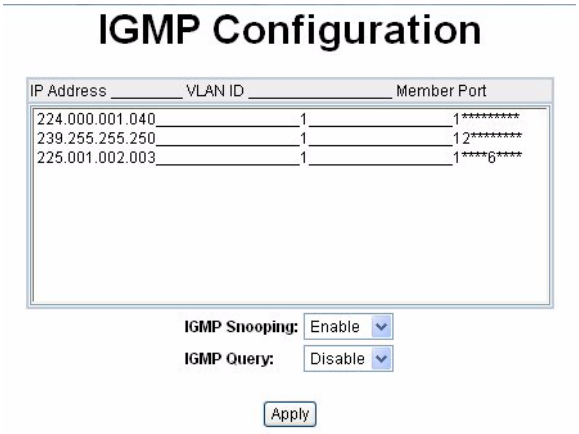


Abbildung 5-35: Oberfläche IGMP-Konfiguration

5.25.2 X-Ring

Der X-Ring bietet schnellere, redundante Wiederherstellung als die Spanning-Tree-Topologie. Die Vorgehensweise ist ähnlich wie bei STP oder RSTP, aber die Algorithmen sind unterschiedlich.

In der X-Ring-Topologie sollte die X-Ring-Funktion für jeden Switch aktiviert sein. Weiterhin werden jedem Switch zwei Ports auf dem Ring zugewiesen. Nur ein Switch in der X-Ring-Gruppe wird als Backup-Switch definiert. Wird einer von zwei Member Ports blockiert, so bezeichnet man diesen als Backup-Port. Der andere Port wird als Working Port (arbeitender oder aktiver Port) bezeichnet. Die anderen Switches werden als Working Switches bezeichnet und ihre beiden Member Ports jeweils als Working Ports. Wenn die Netzwerkverbindung ausfällt, dann wird der Backup-Port automatisch zu einem Working Port, um den Ausfall abzufangen.

Der Switch kann als Ring Master oder Slave konfiguriert werden. Der Ring Master hat die Berechtigung, Parameter auszuhandeln und Befehle an die anderen Switches in der X-Ring-Gruppe zu geben. Arbeiten zwei oder mehr Switche

im Master Mode, dann wählt die Software den Switch mit der niedrigsten MAC-Adresse als Ring Master aus.

Das System unterstützt auch den Koppelring, der zwei oder mehr X-Ring-Gruppen für ein redundantes Backup miteinander verbindet, sowie die Dual-Homing-Funktion, welche Verbindungsverluste zwischen den X-Ring-Gruppen und den Upper Level/Core Switches verhindert.

- ***Enable X - ring:*** Aktiviert die X-Ring-Funktion.
- ***Enable Ring Master.:*** Aktiviert den Switch als Ring Master.
- ***1ST & 2ND Ring Ports:*** Zwei Ports werden als Member Ports ausgewählt. Einer der Ports wird als Working Port und der andere als Backup-Port definiert. Das System wählt automatisch den Working Port und den Backup Port aus.
- ***Enable Coupling Ring:*** Aktiviert die Koppelring-Funktion.
- ***Coupling port:*** Hier wählen Sie einen Member Port aus.
- ***Control port:*** Wählt den Switch als Master Switch im Koppelring aus.
- ***Enable Dual Homing:*** Aktiviert die Dual-Homing-Funktion. Wählen Sie einen Port am Switch als Dual Homing Port aus. In einer X-Ring-Gruppe gibt es jeweils nur einen Dual Homing Port. Dual Homing ist nur möglich, wenn die X-Ring-Funktion aktiviert worden ist.
- Klicken Sie auf **Apply**.

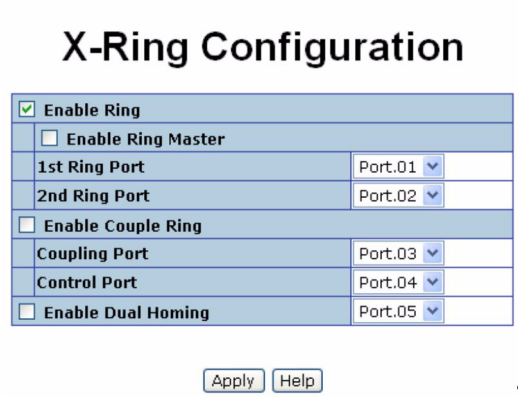


Abbildung 5-36: Oberfläche X-Ring

Hinweis

Wurde die X-Ring-Funktion aktiviert, dann muss RSTP deaktiviert sein.

5.26 Sicherheitskonfiguration

5.26.1 802.1X-Konfiguration

802.1x ist ein Standard, der die Authentifizierung gemäß IEEE spezifiziert und es einem Client ermöglicht, eine Verbindung zu einem Funk-Access-Point oder einem verkabelten Switch aufzubauen. Der Standard verhindert, dass einem Client Zugriff zum Netzwerk gewährt wird, solange er dazu nicht seine Zugangsberechtigung nachgewiesen hat. Dies erfolgt z.B. in Form eines Benutzernamens und eines Passworts, welche von einem separaten Server verifiziert werden.

Systemkonfiguration Hier konfigurieren Sie die Parameter der IEEE 802.1X-Funktion.

- ***IEEE 802.1x PROTOCOL:*** Aktiviert bzw. deaktiviert das 802.1x-Protokoll.
- ***RADIUS SERVER IP:*** Legt die IP-Adresse des Radius Servers fest.
- ***SERVER PORT:*** Legt den UDP-Zielport fest, der bei Authentifizierungsanfragen an den angegebenen Radius Server verwendet wird.
- ***ACCOUNTING PORT:*** Legt den UDP-Zielport fest, der bei Abrechnungsanfragen an den angegebenen Radius Server verwendet wird.
- ***SHARED KEY:*** Legt einen Verschlüsselungsschlüssel fest, der bei der Authentifizierung mit dem angegebenen Radius Server verwendet wird. Dieser Schlüssel muss dem Verschlüsselungsschlüssel auf dem Radius Server entsprechen.
- ***NAS, IDENTIFIER:*** Legt die Kennung für den Radius Server fest.
- Klicken Sie auf **Apply**.

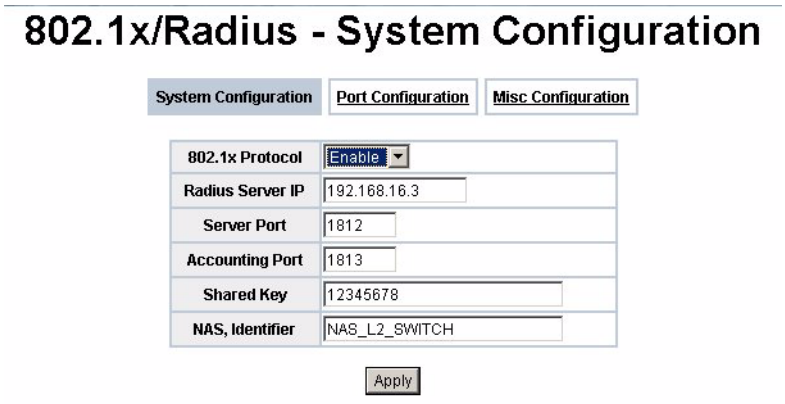


Abbildung 5-37: Oberfläche zur 802.1x-Systemkonfiguration

802.1x-Konfiguration pro Port

Hier können Sie den 802.1x-Authentifizierungsstatus für jeden Port konfigurieren.

- ***REJECT:*** Der angegebene Port muss in einem nicht-autorisierten Zustand verbleiben.

- ***ACCEPT:*** Der angegebene Port muss in einem autorisierten Zustand verbleiben.
- ***AUTHORIZED:*** Der angegebene Port wird entweder in den Zustand "autorisiert" oder "nicht-autorisiert" geschaltet. Der Zustand hängt von Ergebnis des Authentisierungsprozesses ab, der zwischen dem Supplicant und dem Authentisierungsserver durchgeführt wird.
- ***DISABLE:*** Der angegebene Port muss in einem autorisierten Zustand verbleiben.
- Klicken Sie auf **Apply**.

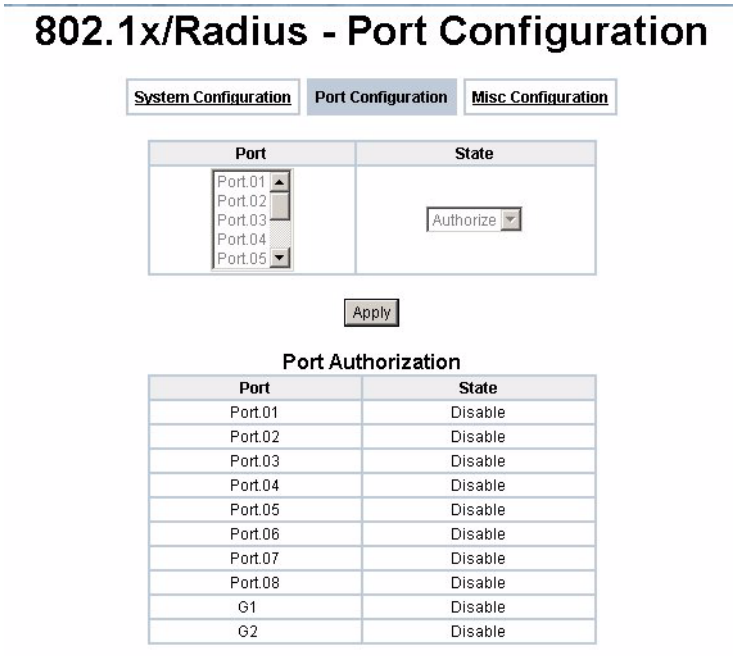


Abbildung 5-38: Oberfläche zur 802.1x-Konfiguration pro Port

Verschiedene Konfigurationen

- ***QUIET PERIOD:*** Legt die Zeitspanne fest, während welcher der Port keine Anfrage entgegennimmt.
- ***TX PERIOD:*** Legt die Zeitspanne fest, während welcher der Port darauf wartet, während einer Authentifizierung die nächste EAPOL PDU zurückzusenden.
- ***SUPPLICANT TIMEOUT:*** Legt die Zeitspanne fest, die der Switch auf die Antwort des Supplicants auf eine EAP-Anfrage wartet.
- ***SERVER TIMEOUT:*** Legt die Zeitspanne fest, die der Switch auf die Antwort des Servers auf einen Authentifizierungs-Anfrage wartet.
- ***MAX REQUESTS:*** Legt die Anzahl der Authentisierungsversuche fest, nach denen die Authentisierung als fehlgeschlagen gilt und die Authentisierungssitzung beendet wird.
- ***REAUTH PERIOD:*** Legt die Zeitspanne fest, nach der angebundene Clients erneut authentisiert werden müssen.
- Klicken Sie auf **Apply**.

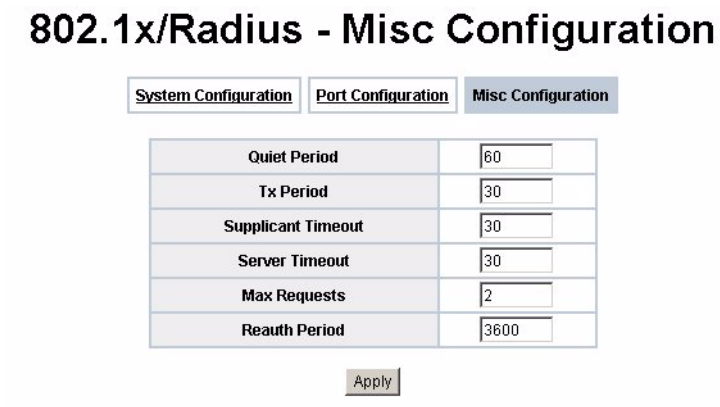


Abbildung 5-39: Oberfläche zu verschiedenen Konfigurationen gemäß 802.1x

5.26.2 Port-Sicherheit

Benutzen Sie die MAC-Adresse, um die Sicherheit des Ports zu gewährleisten.

Statische MAC-Adressen

Fügen Sie eine statische MAC-Adresse hinzu, welche in der Adresstabelle des Switch angegeben wird. Es spielt hier keine Rolle, ob das Gerät physikalisch an den Switch angebunden ist oder nicht. Der Switch muss dann nicht noch einmal die MAC-Adresse des Geräts erlernen, wenn dieses wieder im Netzwerk betrieben wird, nachdem die Verbindung abgebrochen wurde oder das Gerät ausgeschaltet wurde.

Hinzufügen der statischen MAC-Adresse

- ***MAC ADDRESS:*** Geben Sie die MAC-Adresse des Ports ein, die permanent den Datenverkehr weiterleitet, unabhängig von der Aktivität des Geräts im Netzwerk.
- ***PORT NO.:*** Öffnen Sie das Auswahlmenü, um die Portnummer auszuwählen.
- ***VLAN ID:*** Geben Sie die VLAN ID zur MAC-Adresse ein, sofern die MAC-Adresse zu einer VLAN-Gruppe gehört.
- Klicken Sie auf **Add**.
- Um die MAC-Adresse aus der Filtertabelle zu löschen, wählen Sie die MAC-Adresse aus und klicken auf die Schaltfläche **Delete**.

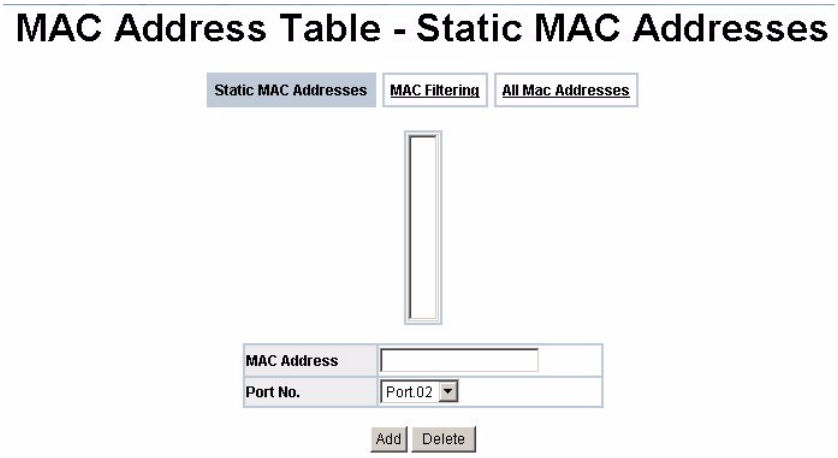


Abbildung 5-40: Oberfläche zur Konfiguration statischer MAC-Adressen

Filtern von MAC-Adressen

Durch Filtern der MAC-Adressen kann der Switch einfach vorkonfigurierte MAC-Adressen herausfiltern und so Sicherheitslücken reduzieren.

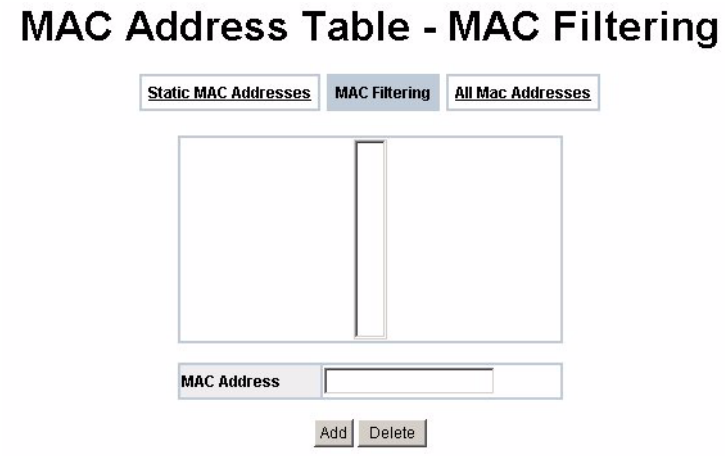


Abbildung 5-41: Oberfläche zum Filtern von MAC-Adressen

- ***MAC ADDRESS:*** Geben Sie die MAC-Adresse ein, die Sie herausfiltern wollen.
- ***VLAN ID:*** Geben Sie die VLAN ID zur MAC-Adresse ein, sofern die MAC-Adresse zu einer VLAN-Gruppe gehört.
- Klicken Sie auf **Add**.
- Um die MAC-Adresse aus der Filtertabelle zu löschen, wählen Sie die MAC-Adresse aus und klicken auf die Schaltfläche **Delete**.

Alle MAC-Adressen

Prüfen Sie die MAC-Adresse des Geräts, das an diesem Port angeschlossen ist, sowie die MAC-Adressen der übrigen angebundenen Geräte.

- Wählen Sie den Port aus.
- Die Informationen zur statischen MAC-Adresse des ausgesuchten Ports werden angezeigt.
- Klicken Sie danach auf die Schaltfläche **Clear MAC Table**, um die auf dem Bildschirm dargestellten Informationen zu den statischen MAC-Adressen der ausgesuchten Ports zu löschen.

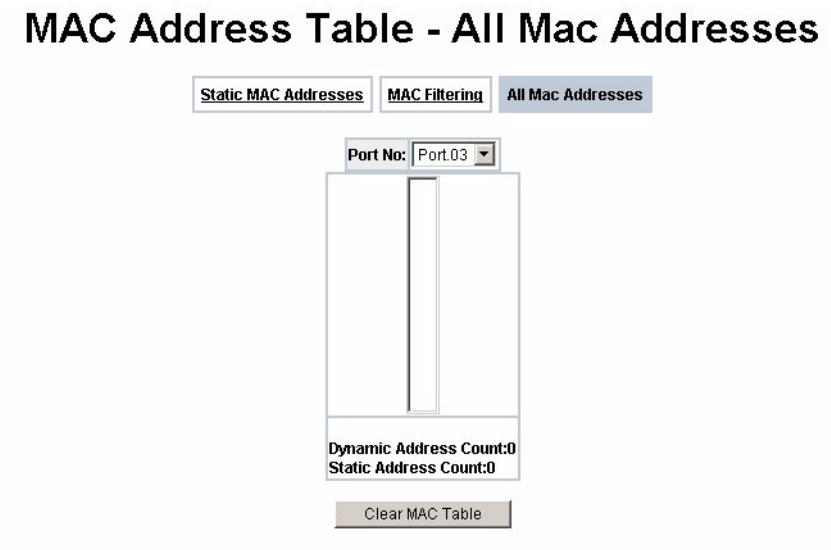


Abbildung 5-42: Oberfläche alle MAC-Adressen

5.27 Power-over-Ethernet

Dieser Abschnitt beschreibt die PoE-Funktion.

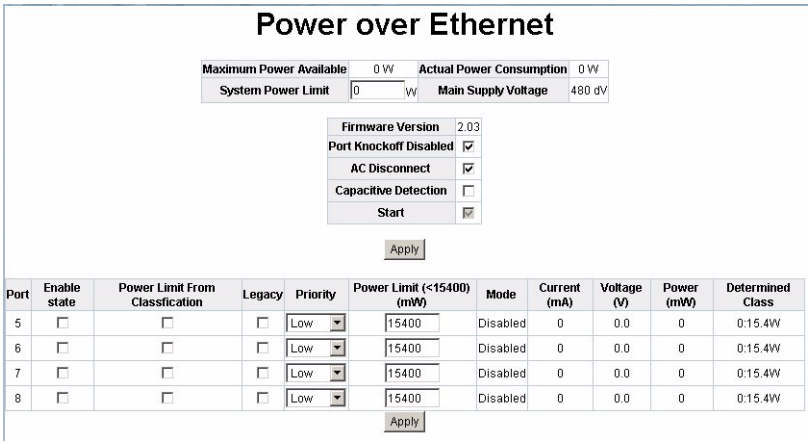

Power over Ethernet
Maximum Power Available 0 W
Actual Power Consumption 0 W
System Power Limit 0 W
Main Supply Voltage 480 dV
Firmware Version 2.03
Port Knockoff Disabled
AC Disconnect
Capacitive Detection
Start
Apply
Port Enable state Power Limit From Classfication Legacy Priority Power Limit (<15400) (mW) Mode Current (mA) Voltage (V) Power (mW) Determined Class
5 Low 15400 Disabled 0 0.0 0 0:15.4W
6 Low 15400 Disabled 0 0.0 0 0:15.4W
7 Low 15400 Disabled 0 0.0 0 0:15.4W
8 Low 15400 Disabled 0 0.0 0 0:15.4W
Apply

Abbildung 5-43: Oberfläche Power-over-Ethernet

- ***Maximum Power Available:*** Zeigt die maximal einzuspeisende Netzspannung in Watt an.
- ***Actual Power Consumption:*** Diese Spalte zeigt die tatsächliche Leistungsaufnahme an.
- ***Power Source:*** Diese Spalte zeigt die Spannungsquelle an, die das Gerät mit Netzspannung versorgt.
- ***Power Source 1 (AC):*** Diese Spalte zeigt die Stromversorgung über Spannungsquelle 1 an.
- ***Power Source 2 (AC+DC):*** Diese Spalte zeigt die Stromversorgung über Spannungsquelle 2 an (modellabhängig).
- ***Firmware Version:*** Diese Spalte zeigt die Firmware-Version an.
- ***AC Disconnect:*** Wählen Sie dieses Ankreuzfeld aus, um die Stromzufuhr (Wechselstrom) abzuschalten.

- ***Capacitive Detection:*** Wählen Sie dieses Ankreuzfeld aus, um die Stromversorgung des angeschlossenen Geräts anzuzeigen.
- Klicken Sie auf die Schaltfläche **Apply**, um die Einstellung zu aktivieren.
- Klicken Sie auf **Refresh**, um den Status aller Spalten zu aktualisieren.
- ***Port:*** Index der PoE-Ports.
- ***Enable State:*** Prüfen Sie den Status, um die PoE-Funktion des Ports zu aktivieren.
- ***Power Limit From:*** Prüfen Sie die Einstellungen, um die Begrenzung der Netzspannung auszuwählen.
  - Classification: Wenn dieses Ankreuzfeld ausgewählt wurde, begrenzt das System die dem angeschlossenen Gerät gelieferte Netzspannung entsprechend der eingestellten Klassifizierung.
  - Management: Wenn dieses Ankreuzfeld ausgewählt wurde, dann kann der Benutzer die anliegende Netzspannung manuell begrenzen.
- ***Legacy:*** Prüfen Sie die Einstellungen, um die bereits vorhandenen Geräte weiter unterstützen zu können.
- ***Priority:*** Öffnen Sie das Auswahlmenü, um die Priorität der Spannungsversorgung festzulegen.
- ***Port Limit (<15400) mW:*** Wenn die Option *Power Limit From* auf den *Management*-Modus eingestellt ist, kann der Benutzer hier Werte zur Begrenzung der Netzspannung eingeben, die unter 15,4 Watt liegen müssen.
- ***Mode:*** Zeigt den Betriebszustand des Ports an.
- ***Current (mA):*** Zeigt die Stromzufuhr zum Port an.
- ***Voltage (V):*** Zeigt die Betriebsspannung des Ports an.
- ***Power (mW):*** Zeigt die Leistungsaufnahme des Ports an.
- ***Determined Class:*** Zeigt die Begrenzungsklasse der Netzspannung an.
- Klicken Sie auf die Schaltfläche **Apply**, um die Einstellung zu aktivieren.

5.28 Standardeinstellungen

Reset-Schalter zum Zurücksetzen auf die Standardkonfiguration.

- Klicken Sie auf die Schaltfläche **Default**, um alle Einstellungen auf die Standardwerte zurückzusetzen.

Abbildung 5-44: Oberfläche Standardeinstellungen

5.29 Konfiguration abspeichern

Speichert alle Konfigurationen ab, die Sie in dem System vorgenommen haben.

- Klicken Sie auf die Schaltfläche **Save Flash**, um die Änderungen im Flash Memory abzuspeichern

Abbildung 5-45: Oberfläche Konfiguration abspeichern

5.30 System neu starten

Starten Sie den Switch durch ein Software Reset neu.

- Klicken Sie auf die Schaltfläche **Reboot**, um das System neu zu starten.

Abbildung 5-46: Oberfläche zum System-Neustart

6 Fehlerbehebung

Dieser Abschnitt soll Ihnen helfen, die häufigsten Probleme zu lösen, die beim Betrieb des funkwerk S128p FastEthernet PoE Switch auftreten.

6.1 Falsch angeschlossene Verbindungen

Der Switch Port ist in der Lage, eine automatische Erkennung von geraden Kabeln oder gekreuzten Kabeln durchzuführen, wenn Sie den Switch mit anderen Ethernet-Geräten verbinden. An dem RJ-45-Netzanschluss muss ein entsprechendes UTP- oder STP-Kabel angeschlossen sein. Am 10/100 Mbit/s-Port werden vieradrige Twisted-Pair-Kabel angeschlossen, am Gigabit 1000T Port achtadrige Twisted-Pair-Kabel. Wird der RJ-45-Stecker nicht am richtigen Pin eingesteckt, dann kann keine Verbindung aufgebaut werden. Bei einer Glasfaserverbindung sollten Sie darauf achten, dass der Modus des Glasfaserkabels und des Glasfasermoduls übereinstimmen.

Fehlerhafte oder lockere Kabel

Achten Sie darauf, dass die Kabel nicht zu locker eingesteckt sind und dass keine schadhaften Kabel verwendet werden. Wenn die Kabel in Ordnung sind, dann stellen Sie sicher, dass die Verbindungen einwandfrei eingesteckt und verlegt sind. Wenn Sie damit nicht das Problem beheben können, versuchen Sie es mit einem anderen Kabel.

Nicht-standardisierte Kabel

Kabel, die nicht dem Standard entsprechen oder bei denen die Aderbelegung falsch ist, sind oft für Netzwerkausfälle, Stillstände oder andere Netzwerkprobleme verantwortlich. Sie können die Leistungsfähigkeit Ihres Netzwerks stark einschränken. Wir empfehlen bei jeder Installation eines 100Base-T-Netzwerks den Kategorie-5-Kabeltester als bewährtes Werkzeug zur Kabelüberprüfung einzusetzen.

RJ-45 Ports: Verwenden Sie ungeschirmte Twisted-Pair-Kabel (UTP) oder geschirmte Twisted-Pair Kabel (STP) für RJ-45-Verbindungen: 100 Ω Kategorie 3, 4 oder 5 Kabel für 10 Mbit/s-Verbindungen oder 100 Ω Kategorie 5 Kabel für 100 Mbit/s-Verbindungen. Stellen Sie weiterhin sicher, dass keine Twisted-Pair-Verbindung länger als 100 m ist. Für Gigabit Ports müssen Sie Kategorie

5 oder 5e Kabel für Verbindungen mit einer Datenrate von 1000 Mbit/s verwenden. Die Kabellänge darf 100m nicht überschreiten.

Fehlerhafte Netzwerktopologien

Stellen Sie unbedingt sicher, dass Sie mit einer zulässigen und funktionierenden Netzwerktopologie arbeiten. Häufige Fehlerquellen in der Topologie sind überlange Kabelstrecken und der Einsatz von zu vielen Repeatern (Hubs) zwischen den Endknoten. Sie sollten weiterhin sicherstellen, dass Ihre Netzwerktopologie keine Schleifen auf den Datenpfaden bildet. Zwischen zwei Endknoten sollte es immer nur eine aktive Verkabelung geben. Schleifen auf Datenpfaden führen zu Broadcast Storms und beeinträchtigen damit stark die Leistungsfähigkeit Ihres Netzwerks.

6.2 Fehleranzeige durch LEDs

Der Switch kann auf einfache Art und Weise mittels der LEDs am Gerät überwacht werden. Sie zeigen die gängigen Probleme an, mit denen der Benutzer konfrontiert werden kann, und helfen ihm, die Probleme zu erkennen und zu lokalisieren.

Wenn die LED für die Netzspannung nicht leuchtet, obwohl das Stromkabel eingesteckt ist, dann ist möglicherweise die Steckdose oder das Stromkabel defekt. Verliert der Switch jedoch Netzspannung, nachdem er bereits gelaufen ist, dann sollten Sie überprüfen, ob sich Kabel gelöst haben oder ob Spannungsverluste oder Überspannungen an der Steckdose auftreten. Kann das Problem auch dann noch nicht gelöst werden, sollten Sie sich an Ihren Händler wenden.

7 Technische Daten

Dieser Abschnitt beschreibt die technischen Daten zum **funkwerk S128p FastEthernet PoE Switch**.

STANDARD	IEEE802.3 10BASE-T IEEE802.3u 100BASE-TX IEEE802.3z Gigabit Fiber (Gigabit Glasfaser) IEEE802.3ab 1000Base-T IEEE802.3x Flow Control and Back Pressure IEEE802.3ad Port Trunk with LACP (3ad-Port-Leitung mit LACP) IEEE802.1d Spanning Tree Protocol IEEE802.1w Rapid Spanning Tree IEEE802.1p Class of Service IEEE802.1Q VLAN Tagging IEEE 802.1x User Authentication (Benutzerauthentisierung) IEEE 802.3af Power over Ethernet
LED-ANZEIGEN	Netzspannung (grün) 10/100TX Port: Link/Activity (grün) Vollduplex/Kollision (orange), 100 Mbit/s (grün) Forwarding /Detect (Weiterleiten / Erkennen) (grün) Gigabit Kupfer-Port: 1000/100 Mbit/s (grün/orange) Link/Activity (grün), Vollduplex/Kollision (orange) Mini GBIC: Link/Activity (grün)

NETZWERKANSCHLÜSSE	100Base-T: RJ-45-Anschluss mit Auto-MDI/MDI-X. Port 5 - 8 unterstützen POE Inject-Funktionalität. 1000Base-T: RJ-45-Anschluss mit Auto-MDI/MDI-X. Gigabit Glasfaser: MINI GBIC-Anschlussdose.
SWITCHARCHITEKTUR	Store-and-Forward Switch-Architektur Datenrate bis zu 8,3 Mbit/s
BACKPLANE	5,6 Gbit/s
MAC-ADRESSEN	8 K MAC-Adresstabelle mit Auto-Learning-Funktion
FLASH ROM	4 Mbyte
DRAM	32 Mbyte
PAKET-PUFFERSPEICHER	1 Mbit/s für Paket-Pufferspeicher
STROMVERSORGUNG	100 - 240V Wechselstrom, 50/60 Hz
LEISTUNGSAUFNAHME	73 Watt für das System (Maximalwert)
BELÜFTUNG	1 Lüfter
BETRIEBSUMGEBUNGSTEMPERATUR	0°C - 45°C, 5% - 95% relative Luftfeuchtigkeit
LAGERUNG	-40°C - 70°C, 95% relative Luftfeuchtigkeit
ABMESSUNGEN	217 mm (B) x 140 mm (T) x 43 mm (H)
EMI	Konform zu FCC Klasse A, CE
SICHERHEIT	UL cUL CE/EN60950-1

8 Anhang

8.1 Pinbelegung am Konsolenport

Der serielle DB-9 Port dient dazu, den Switch bei einer Out-of-Band-Konfiguration anzubinden. Der Zugriff auf das menügeführte Konfigurationsprogramm ist von einem Endgerät aus möglich oder von einem PC, auf dem ein Endgerät emuliert wird. Die Pinbelegungen, die für Verbindungen auf den seriellen Ports verwendet werden können, sind in den folgenden Tabellen angegeben.

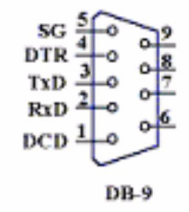


Abbildung 8-1: Pinnummern am DB-9-Konsolenport

- Pinbelegung am DB-9-Konsolenport

EIA-Schaltkreis	CCITT-Signal	Beschreibung	Switch: DB9 DTE Pin Nr.	PC DB9DTE Pin Nr.
BB	104	RxD (empfangene Daten)	2	2
BA	103	TxD (übertragene Daten)	3	3
AB	102	SGND (Signal Erde)	5	5

- Verbindung von Konsolenport zu 9-Pin Endgerätport auf PC

Switch: 9-Pin serieller Port	CCITT-Signal PC 9-Pin	Endgerätport
2 RXD	<---------RXD ----------	3 TxD
3 TXD	----------TXD ---------->	2 RxD
5 SGND	----------SGND ----------	5 SGND

8.2 Kabel

Die RJ-45 Ports auf dem Switch unterstützen den automatischen MDI/MDI-X-Betrieb. Sie können daher standardisierte 1:1 Twisted-Pair-Kabel verwenden, um andere Netzwerkgeräte anzuschließen (PCs, Server, Switche, Router oder Hubs). Bitte beachten Sie die Kabelspezifikationen in der folgenden Tabelle.

- Kabeltypen und Spezifikationen

Kabel	Typ	Maximale Länge	Netzwerkanschlüsse
10BASE-T	Kat. 3, 4, 5100 Ohm	UTP 100 m	RJ-45
100BASE-TX	Kat. 5 100 Ohm UTP	100 m	RJ-45
100BASE-FX	50/125 oder 62,5/125 Mikrometer Kern Multimode-Glasfaser (MMF)	2 km	SC oder ST

Tabelle 8-1: Tabelle: Kabelspezifizierungen

8.3 100BASE-TX/10BASE-T Pinbelegung

Bei 100BASE-TX/10BASE-T-Kabeln werden Pin 1 und 2 zur Datenübertragung verwendet. Beim Einsatz von PoE dienen Pin 3 und 6 dienen zum Datenempfang, während Pin 4, 5, 7 und 8 für die Netzspannung sorgen.

8.3.1 RJ-45 Pinbelegung von PD, die nicht dem 802.3af Standard PD entsprechen, mit feldkompatibler POE HUB RJ-45 Pinbelegung

- Pinbelegung eines Cisco PD, nicht konform zu Standard 802.3af

Pin	Signal
1	RX+
2	RX-
3	TX+
4	VCC -
5	VCC -
6	TX-
7	VCC +
8	VCC +

- Pinbelegung eines feldkompatiblen PoE Hubs

Pin	Signal / Name
1	RX+
2	RX-

Pin	Signal / Name
3	TX+
4	VCC+
5	VCC+
6	TX-
7	VCC-
8	VCC-

Hinweis

Das "+" und "-" Zeichen zeigen die Polarität der Adern an, die jeweils ein Adernpaar bilden. Bevor Sie Ihr PD in Betrieb nehmen, sollten Sie die Pinbelegung der RJ-45-Netzwerkanschlüsse überprüfen. Sie sollten dem Standard IEEE802.3af entsprechen. Ist dies nicht der Fall, müssen Sie eventuell die Pinbelegung eines RJ-45-Netzwerkanschlusses ändern, an den Sie das UTP-Kabel anschliessen möchten.

Alle Ports auf diesem Switch unterstützen den automatischen MDI/MDI-X-Betrieb. Sie können daher 1:1-Kabel verwenden, um andere PCs, Server, Switches oder Hubs anzuschließen. Bei 1:1-Kabeln werden Pin 1, 2, 3 und 6 am einen Kabelende Ende-zu-Ende mit Pin 1, 2, 3 und 6 am anderen Kabelende verbunden. Die folgende Tabelle zeigt die Pinbelegungen für 10BASE-T/ 100BASE-TX MDI und MDI-X Ports

Pin MDI-X	Signalbezeichnung	MDI Signalbezeichnung
1	Receive Data (empfange Daten) plus (RD+)	Transmit Data (übertrage Daten) plus (TD+)
2	Receive Data (empfangene Daten) minus (RD-)	Transmit Data (übertragene Daten) minus (TD-)
3	Transmit Data (übertragene Daten) plus (TD+)	Receive Data (empfangene Daten) plus (RD+)
6	Transmit Data (übertragene Daten) minus (TD-)	Receive Data (empfangene Daten) minus (RD-)